

Building Technologies Technical Reference Guide

Version 1.2

September 29, 2016



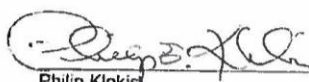
Version History / Change Record

Revision	Chapter	Change
Revision 1.1	1	TIC
	1	Formal Security Evaluation
	1	Security Evaluation Criteria
	1	Devices Risk Assessments
	1	Scanned Device List
	1	Client Software (Non-Standard Software)
	1	Non-standard software on GSA servers
	1	GSA IT Security Scanning Process
	1	Building Systems Network (BSN)
	2	BACnet
	3	Cabling Installation Options
	3	Overview of Data Circuit Installation
	4	Responsibilities respective to server and application support
	4	Server Installation Guidelines
	4	Methods for Remotely Accessing a PBS Technical Operations Server
	4	System Documentation and Monitoring

	4	Backup Solutions
	4	Planned/Unplanned Outages and Maintenance
	6	Reporting an BMC Issue
	6	BMC support system workflow
	7	PACS (new chapter)
Revision 1.2	1	Introduction
	1	Scanning Process
	1	What is BSN?
	1	No external/commercial network connections allowed
	1	Incident Response and Disaster Recovery
	2	Issues with daisy chaining switches
	4	Solution Architecture and Requirements Analysis
	4	Server Standards
	4	Application Installation and Maintenance Guidelines
	4	Server Access
	4	Methods for Remotely Accessing a PBS Technical Operations Server
	4	System Documentation and Monitoring
	4	How to request Remote Desktop User Access

	4	How to request Administrator Access
	4	Copying Files to a Server on the BSN
	4	Methods for Remotely Accessing a PBS Technical Operations Server
	5	New SOW format and language
	6	Reporting an BMC Issue
	6	PBS Technical Operations Team
	6	BMC Outage Process
	6	BMC Admin, RDP, and Reboot Process
	6	SFTP (Secure File Transfer Protocol) Request Process
	6	SMTP Email Server Information
	7	Physical Access Controls Systems (new chapter)
	8	Best Practices (new chapter)

Approvals



Philip Klokist
Associate CIO
Office of Chief Information Officer, Public Buildings IT Services
GSA IT



Kurt Garbars
Senior Agency Information Security Officer (SAISO)
GSA IT

Stephen Sakach
Assistant Commissioner
PBS Office of Facilities Management

LAURA
STAGNER

Digitally signed by LAURA STAGNER
DN: cn=U.S. Government, ou=General
Services Administration, o=LAURA STAGNER,
c=US, email=LAURA.STAGNER@GSA.GOV,
Date: 2016.07.29 09:05:27 -0400

Laura Stagner
Assistant Commissioner
PBS Office of Design and Construction



Robert Carter
Associate Administrator
Office of Mission Assurance

Introduction

The nation's buildings are increasingly relying on building control systems with embedded communications technology and many enabled via the Internet. While, the advent of Internet of Thing (IoT) allows ease of use, remote access and data integration, it can also be easy targets for hackers and people with malicious intent. Attackers can exploit these systems to gain unauthorized access to facilities; be used as an entry point to the traditional informational technology (IT) systems and data; cause physical destruction of building equipment; and expose an organization to significant financial obligations to contain and eradicate malware or recover from a cyber-event. Federal facilities include courthouses, laboratories, regional office buildings, many of which are part of the nation's critical infrastructure. These facilities contain building and access control systems such as heating, ventilation, and air conditioning; electronic card readers; and closed-circuit camera systems that are increasingly being automated and connected to other information systems or networks and the Internet. As these systems are becoming more connected, so are their vulnerability to potential cyber-attacks.

As we have learned in recent highly visible cybersecurity incidents at Office of Personnel Management (OPM), Target, Home Depot, Sony and Veterans Affairs, hacking is a growing trend. GSA does not want to be the next target to prove the external threats are real enough to raise concerns.

Cyber incidents can compromise Personally Identifiable Information (PII) and cause outages related to power, network, or other issues that can not only cause major damage to security infrastructure of a building, it can also have a long term repelling effect that can go on for many years.

Building a platform focused on security with disaster recovery in mind, will limit these type of incidents, protecting the infrastructure; including the building systems, which can be caused by internal or external sources.

While physical and cyber security of our buildings is a high priority, GSA also understands there needs to be balance between continuity of operations and vigilance for security. Therefore, as with any business decision, GSA IT and Office of Facilities Management (OFM) will be taking a risk-based decision approach that evaluates exposure, building level, type of vulnerability and actual physical impact/ likelihood, of threat.

The *Building Technologies Technical Reference Guide* was created to protect and enhance the GSA IT posture, and in response to repeated requests for information and formalized guidance related to the technical integration of building monitoring and control (BMC) systems to the GSA network and within its GSA's information technology (IT) environment. BMC systems include, but are not limited to building technologies such as advanced metering systems (AMS), building automation systems, lighting control systems, physical access control systems (PACS), renewable energy systems, and digital signage. These systems, while closely related to the scope of facilities management, are IT systems and do collect GSA building data, and as such are subject to the same Federal and agency specific policies and security standards as any other Federal IT system. It is the intent of this document to not only inform on those policies and standards, but to establish a consistent approach for how these technologies will be implemented

and supported within GSA.

This guide was initiated and published by the Public Buildings Information Technology Services PB-ITS, within GSA IT and developed and reviewed with extensive participation with Office of Mission Assurance, multiple offices of PBS including Facilities Management, Design and Construction, as well as with participants from the Regions. The organization and oversight for this guide was led by a Core Team of senior management from multiple divisions of PBS and included leadership from several GSA Regions. Each chapter of this guide covers a functional area, and the content for each was developed through working group meetings, which included the participation of stakeholders and subject matter experts from central office and the regions.

The Building Technologies Technical Reference Guide is consistent with existing Federal and GSA specific IT policies and is partnered with the [Building Monitoring and Control System Technology Policy](#), which was issued jointly by PB-ITS, Facilities Management and Design & Construction divisions. For guidance on Smart Building implementations and industry best practices, please refer to the [GSA Smart Buildings Program Guide](#) and the [GSA Smart Building Implementation Guide](#).

This guide is a “living document” and will be updated as necessary to accommodate improvements to processes, evolved best practices, and any new or updated policies or standards relevant to the implementation of building monitoring and control systems. Users of this guide are encouraged to provide feedback that will lead to improvement in future versions.

Table of Contents

Version History / Change Record.....	2
Approvals.....	5
Introduction	6
Chapter 1:	12
Policy/Standards & IT Security	12
1.0 Overview	12
1.1 Roles and Responsibilities, BMC Systems	12
1.2 Trusted Internet Connection (TIC).....	13
1.3 Requirements for Network Connection.....	13
1.3.1 Government Furnished Equipment.....	14
1.3.2 Server Security Assessment	14
1.3.3 Device Security Assessment	14
1.4 Non-Standard Software Review Process	16
1.4.1 EARC Evaluation of Non-standard Software.....	17
1.4.2 Non-standard software on GSA workstations.....	18
1.4.3 Non-standard software on GSA servers	18
1.5 Security Assessment and Evaluation Process for BMC Systems Devices	18
1.6 GSA Network Access to Perform Duties	22
1.6.1 HSPD-12 Credentialing and Systems Privileges.....	22
1.7 Building Systems Network (BSN)	23
1.7.1 What is the Building Systems Network (BSN)?	24
1.7.2 Why is the BSN Necessary?.....	24
1.7.3 Who is Responsible for the Creation and Management of the BSN?	24
1.7.4 BSN Implementation.....	25
1.7.5 What Changes Can Be Expected Once the BSN ACL is Applied	25
1.7.6 Will the BSN Be Implemented the Same Way for Every Site?	25
1.7.7 BSN Building Consoles.....	27
1.7.8 Using Citrix and Building Console Workstations	28
1.7.9 Steps to Integrate Sites on to the BSN from the ENT Domain.....	29
1.8 Incident Response and Disaster Recovery	29
1.8.1 Incident Response	29
1.8.2 Disaster Recovery	29

Appendix A: Contact Information	30
Appendix B: Listing of Reference Policies	30
Appendix C: Security for GSA Building Automation Systems.....	32
Appendix D: Top Ten Most Common Vulnerabilities in BMC Systems Scans	34
Chapter 2	42
Network Infrastructure	42
2.0 Overview	42
2.1 Roles and Responsibilities	43
2.1.1 PB-ITS Building and Energy Systems Technical Project Manager	43
2.1.2 GSA-IT's Network Operations (NetOps) Team	43
2.2 Standards for Interoperability	44
2.3 Network Topology	45
2.3.1 Network Design Requirements: Submitting a Network Design Diagram to PB-ITS and NetOps	46
2.3.2 Sample Network Design Diagrams.....	47
2.4 Hardware Standards & Policy	49
2.4.1 Requesting Switches and Routers.....	49
2.4.2 Configuration and Connection of the Switches and the Routers	49
2.5 Acceptance of Non-Standard Hardware	49
2.6 Implementing BACnet	49
2.6.1 What Is BACnet?	49
2.6.2 How Does BACnet Make Use of IP Networks?	49
2.6.3 Key Definitions (BACnet)	50
2.6.4 Considerations and Rule Sets for Implementing BACnet on the GSA Network.....	51
Appendix E	55
Contact Information.....	55
Chapter 3	56
Cabling, Data Circuit Installation and Upgrade	56
3.0 Overview	56
3.1 Applicable Standards for Cabling Infrastructure	56
3.2 Minimum Requirement for Ethernet Cabling	56
3.3 Attenuation Limit.....	56
3.4 How are GSA-IT's Cabling Standards Enforced?	56
3.5 Cabling Installation Options	57
3.5.1 Cabling for New Infrastructure	57
3.5.2 Cabling Infrastructure for Existing or Migrating Systems.....	57
3.6 General Architecture	57
3.7 Cable Installation and Support	57
3.8 Cabling Roles and Responsibilities.....	57
3.9 Overview of Data Circuit Installation	58

3.9.1	Process for Data Circuit Requests & Sites Visits	58
3.9.2	Important Considerations in the Circuit Installation Process	59
3.9.3	Circuit Installation Roles & Responsibilities.....	59
	Appendix F: Contact Information.....	60
	Appendix G: Listing of Reference Policies	60
	Chapter 4:	61
	BMC Systems Workstations, Application Server Provisioning, Installation and Support.....	61
4.0	Overview	61
4.1	About the Technical Operations Team	61
4.2	BMC Server and Workstations	61
4.3	Solution Architecture and Requirements Analysis	62
4.4	Server Standards	63
4.4.1	Server Virtualization.....	63
4.4.2	Server Specifications	64
4.4.3	Server Security Hardening.....	65
4.5	Application Installation and Maintenance Guidelines.....	65
4.5.1	Responsibilities respective to server and application support only:	65
4.5.2	Application Installation Guidelines for Vendors.....	66
4.5.3	Dedicated Server Support During Installation	66
4.6	Server Access	67
4.6.1	Windows Server Access Requirements.....	68
4.6.2	How to request Remote Desktop User Access	68
4.6.3	How to request Administrator Access.....	68
4.6.4	Copying Files to a Server on the BSN	68
4.6.5	Methods for Remotely Accessing a PBS Technical Operations Server	69
4.7	System Documentation and Monitoring	69
4.7.1	Monitoring	70
4.7.2	Backup Solutions	70
4.7.3	Patching	71
4.8	Communications.....	72
4.8.1	Planned Outages and Maintenance	72
4.8.2	Unplanned outages and Maintenance	74
4.8.3	Group Notifications	74
4.9	Roles and responsibilities	75
	Chapter 5	76
	IT Requirements in Scopes of Work (SOWs) for Building Controls Procurements.....	76
5.0	Overview	76
5.1	Instructions	76
5.1.1	Use of Document	76
5.1.2	Small Projects	76

5.1.3 New Construction (Design and Construction)	76
5.2 Scope of Work Language (to be inserted in BAS SOW).....	76
Chapter 6	87
Technical Support for Building Monitoring and Control and Energy Management Systems	87
6.0 Overview	87
6.1 Reporting a BMC Issue	87
6.1.1 Call or Submit an Email to Technical Operations Team.....	87
6.1.2 Call the Helpdesk hotline	88
6.1.3 Submit an IT Helpdesk ticket online with Service Now.....	88
6.1.4 Describing a BMC/BAS/EMS issue	89
6.2 Support Process.....	89
6.2.1 Help Desk Ticket Initiation	89
6.2.2 Managing and Troubleshooting Open Tickets.....	89
6.2.3 Resolving Open Tickets – Roles and Responsibilities	90
6.2.4 Closing Tickets.....	90
6.2.5 BMC Outage Process	91
6.2.6 BMC Admin, RDP, and Reboot Process	93
6.2.7 SFTP (Secure File Transfer Protocol) Request Process.....	94
6.2.8 SMTP Email Server Information	94
Chapter 7:	95
Physical Access Control System (PACS).....	95
7.1 Overview	95
7.2 Support.....	95
7.2.1 Local Support.....	95
7.2.2 Technical Operations Team.....	95
7.3 Roles and Responsibilities	95
7.3.1 Building and Energy (B&E) System Team.....	95
7.3.2 Network Operations Division (NetOps).....	96
7.3.3 Office of Mission Assurance (OMA).....	96
7.4 Network Architecture and Integration	97
7.4.1 Security Overview	97
7.5 PACS Process Flows	98
7.6 Support Tickets	100
Chapter 8	101
Best Practices for BMC Systems Project Implementations.....	101
8.0 Overview	101
8.1 Why Go Virtual?	101
Glossary	104

Chapter 1:

Policy/Standards & IT Security

1.0 Overview

This chapter details the General Services Administration's (GSA) and Public Building Services' (PBS) standards and Information Technology (IT) security policies with respect to the implementation of Building Monitoring and Control (BMC) devices/systems. It documents the comprehensive system requirements related to approved software, standard hardware, network connectivity, user access and security clearances. Additionally, policies and procedures contained herein will guide PBS projects in preparing for assessment and authorization activities required for ALL GSA information systems.

Current policies for assessment and authorization of systems and devices on Public Building networks are based on NIST SP 800-53 rev3. (please note: GSA IT is in transition to using FIPS 200 NIST standard to implement a tailored baseline of NIST SP 800-53 R4, using NIST SP 800-82 to assist in tailoring to address BMC system). GSA IT is currently in the planning and development stages of a Security A&A boundary for the Building Systems Network (BSN) and the BMC systems that fall under that. Additionally, the GSA IT Security team has issued guidance and procedure documents on the assessment process that detail required steps for security assessments, roles and responsibilities and SLAs/time frames for evaluations. These reference documents can be found on [InSite](#)¹.

1.1 Roles and Responsibilities, BMC Systems

The roles and responsibilities of GSA-IT are explained in the following sections:

- **GSA IT-Network Operations (NetOps)**, is responsible for the entire IP transport layer to include all routing and switching equipment and access to IP connectivity. They have command responsibility for the GSA Local Area Network (LAN) and GSA Wide Area Network (WAN). NetOps is the sole provider for any and all IP addresses for devices associated with its network. NetOps is also responsible for managing the Building Systems Network (BSN) and management of the Access Control List (ACL). Please note: the controllers/devices are the responsibility of the vendor.
- **GSA IT Technical Operations (TechOps)**, is responsible for all PBS servers on GSA WAN/LAN, including IT Server Systems in the Regional Offices, PBS Property Management Centers, and GSA buildings, as well as regionally-based IT systems. This includes server hardware, UPS, Operating Systems, databases, server/application services monitoring, data/system backups and restores.

¹ <https://insite.gsa.gov/portal/category/520178>

- **The GSA IT Security team** performs vulnerability assessments on Building Monitoring and Control Components to meet GSA, PBS, and FISMA flaw identification and continuous monitoring requirements. GSA IT Security performs periodic scans of BMC servers as part of compliance validation. Separate hardware/firmware assessments are performed once on devices designated as Building Monitoring and Control components, reporting on the proper configuration of the device on any GSA network, as well as any residual risks associated with use of the device within GSA. The results of the security assessments provide an executive level view for the security posture of each device connected to the GSA network using an IP address and how the identified vulnerabilities can potentially affect other devices/components on the network. Also responsible for facilitating aspects of Authorization control including: authoring the A&A documents, performing risk assessments, managing the system compliance over the life of the ATO and managing the Plan of Action and Milestones (POA&M) items specific to the Building Technologies systems.
- **Regional project teams** (which may include BAS specialists, Contracting Officers, Project Managers, Property Managers...) are responsible for ensuring that any BMC IT system contracted, purchased, owned and/or operated in the Regions adheres to Policy and Implementation guidance within this document and other applicable GSA guides. Also, these teams are to articulate any contractual agreement with the information technology vendor who provides products and/or services to PBS, including hardware, software and Service Level Agreements. Additionally, the Regions are responsible for contacting the PB-ITS Building and Energy Systems team early in the implementation process (prior to contract award) for applicable contract and implementation requirements. They are responsible for the installation, configuration, and management of the application software. In addition, they are to complete the Application Documentation Form for Tech Ops in a timely manner in order to ensure monitoring and backup routines are established. Please see chapter 4 for links to required documents.
- **Vendor/contractor** is responsible for adherence to GSA IT policies, ensuring BMC devices and applications are secure, completing documentation related to the security and support of their application and devices, and for providing maintenance/support of their devices and software.

1.2 Trusted Internet Connection (TIC)

GSA security policy 2100.1J states:

All network devices that are either owned, managed, maintain a connection to a GSA facility, and/or handle GSA data shall be strategically positioned behind a GSA firewall to provide analysis/correlation, management structure, and minimize threats presented by external attacks. TIC will allow GSA to provide the following security functions for any devices connected to GSA networks:

- Monitoring, incident response, vulnerability assessment, vulnerability management, incident reporting, engineering support, and the enforcement of the agency's specific security policy at the hosted facility.
- Trained, qualified, and cleared staff to support security functions 24x7.
- Limited inbound and outbound connections so that only necessary services are allowed.
- Centralized, secured, and unified management of security events in order to protect the integrity of the U.S. Government data and its infrastructure.

Please note: No external/commercial network connections (4G, DSL, or Cable) are allowed in GSA buildings for managing or monitoring of buildings systems. Such connections will be removed upon discovery.

1.3 Requirements for Network Connection

1.3.1 Government Furnished Equipment

Government furnished (GFE) is defined as “equipment that is owned by the government and delivered to, or made available to a contractor” (FAR Part 45) and computer hardware must be used in all cases for PBS IT systems. This applies to all networking infrastructure, servers and workstations provided for Building Managers, associated with Building Monitoring and Control. Vendor provided computer hardware is not allowed to connect to GSA network and can only be used for pre-commissioning purposes (at no point can it access the GSA network). If vendor provided devices, workstations or servers are discovered, they can be removed without warning.

- **Network equipment-** includes any equipment that has IP routing and switching functionality.
- **Computer hardware-** includes, but is not limited to servers, PCs, laptops and their peripherals (monitors, mice and keyboards). As buildings are integrated with the GSA network, GSA IT will make every effort to provide one desktop and/or one laptop to newly integrated (to the GSA network) sites for the purposes of giving building management staff access to their building monitoring and control system application interfaces. Please note: availability of hardware is dependent on the availability of budgeted funds dedicated for this purpose, which may or may not be renewed on an annual basis. Existing GSA workstation refreshes will still be coordinated through regional GSA-IT manager's office. No hardware (workstations, servers, switches) will be provided unless an approved network diagram is submitted. Please see chapter 2 details about network diagram requirements and submittal.

1.3.2 Server Security Assessment

GSA IT Security currently performs Operating System (OS) scan of the BMC Systems servers. Critical and high vulnerabilities need to be addressed within 30 days. While some of the vulnerabilities are mitigated via routine monthly patching done on the servers by GSA IT, other vulnerabilities, such as multiple version of JAVA, require assistance from property management staff and O&M, responsible for the server. GSA IT Security will also be performing scans of the BMC Systems applications, in the coming months. Application-related security vulnerabilities will also require vendor engagement in order to be mitigated in a timely manner.

1.3.3 Device Security Assessment

All IP addressable devices, appliances or servers that will communicate over the GSA network must be scanned by GSA-IT Security. Before any hardware, software or IT device/system is connected to its network, a security risk assessment of selected management, operational, and technical security controls is performed, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. A security assessment report is produced by GSA IT Security once the device has been assessed, which will be provided to the PBS stakeholders and the vendor. The assessment report will allow GSA to understand and accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. The contractor/vendor must therefore be held responsible for mitigating all security risks identified. Vulnerabilities must be mitigated within the appropriate timeframe as described in the Security Assessment Report mitigation plan along with milestones and timelines for remediation for consideration of GSA-IT in order to connect to the GSA network. GSA IT only needs to scan a certain model device once and not for each project. Once the device has completely gone through the remediation process and has a remediation/hardening plan in place, all other projects

can use that report to configure the named device accordingly.

Please see Appendix D for "Top Ten Most Common Vulnerabilities in BMC Systems Scans"

- **Security Evaluation Criteria** -The GSA IT Security team performs security control reviews utilizing a systematic, repeatable approach, which is utilized to uniformly evaluate any device, application or general support system.
 - The security team reviews basic documentation, performs vulnerability scans, evaluates all items received, and provides feedback to the PBS Requesting Official throughout the review process. Upon completion of the security review the security team is able to determine the extent to which the security controls associated with the device/application (information system) are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the established security requirements.
 - The security team works closely with the vendor/manufacturer or the designated device POC, to addresses the security vulnerabilities by reducing or eliminating them as appropriate.
 - Upon successful completion of the security review, GSA will have the information needed to determine the risk to agency operations, agency assets, or individuals—and thus, will be able to render an appropriate security decision for the information system.
 - GSA IT Security assesses the risk this family of devices poses to the GSA network. Through vulnerability scanning and reviewing available documentation, the Security team provides a holistic security assessment describing the security posture of such devices. At the discretion of the GSA IT Security's office, Device scanning will be performed either in the Central Office testing lab, in Washington DC, or in instances where shipping a device is not practicable, on-site via GSA Site Remote Scanning will be performed.
 - The GSA IT Security team performs a security evaluation then provides a Security Assessment Report (SAR) to the appropriate Point(s) of Contact and/or device stakeholders.
 - Contact the GSA-IT Security Team BMC.IT.Security@gsa.gov to request the Scanning Request Form and other information you may need.

- **Encryption**

The Federal Information Processing Standard (FIPS) 140-2 (see Appendix B) is a U.S. government computer security standard used to accredit cryptographic modules, which is necessary in order to maintain the confidentiality and integrity of the information system. Once a system has been designed and deployed using FIPS compliant technologies it must be operated following documented procedures to ensure keys are created, stored, retired, revoked and otherwise managed in a consistent and secure manner. All file/data transfers inbound to or outbound from the device or software must be encrypted using FIPS 140-2 compliant protocols, all transfers require user authentication, and the authentication credentials must be encrypted during transmission. Lastly, Control and Monitoring of device operations are to be treated as File Transfer functionality

- **Wireless**

All wireless solutions must adhere to the "2100.2B CIO P GSA Wireless Local Area Network (LAN) Security" guide, which mostly covers 802.11 solutions. Additionally, other

non- 802.11 wireless solutions are required to be scanned, remediated, and the solutions evaluated and approved by GSA IT Security in advance of any implementation.

- **SFTP (Secure File Transfer Protocol) Data Transmission**

GSA IT has a standard process and a dedicated SFTP for data transmissions. Please see chapter 4 for more details.

- **Scanned Device List**

All vendor-provided hardware/controllers and application software must be assessed by GSA IT Security. As items get evaluated by the GSA-IT Security team and receive favorable concurrence by the IT Security Team, they will be added to the [Scanned Device List](#). PBS associates can find the current scanned list at the link above. The list is not to be used either for inclusion or exclusion of listed components and is only provided as a guide to devices that have completed favorable assessments. Please note: this is not to be confused with Government Furnished Equipment (GFE) which is defined in section 1.3.1.

1.4 Non-Standard Software Review Process

Non-standard software is referred to applications that cannot be readily downloaded from the GSA Software Delivery agent, referred to as “DSM”. All non-standard software, that has not yet been assessed by GSA IT, will need to go through the evaluation process. GSA IT performs an assessment of the non-standard, which focuses on ensuring software (workstation or server) are currently supported, are generally secure and free of vulnerabilities

The following is an excerpt from [CIO 2160.1D GSA IT Standards Policy v8](#) , which has been tailored for BMC systems applications use:

- GSA Order CIO 2160.1D requires GSA's technology architecture to be based on approved technologies contained in the GSA IT Standards Profile. As such, the GSA Chief Information Officer (CIO) has aligned the IT standards management process with the Agency IT Governance process. The purpose of this is to promote principles of security, performance, innovation, interoperability, efficiency, resource sharing, and sustainability.
- Information technologies can only be used in GSA's IT environment when approved by GSA IT after it has been reviewed against all relevant IT standards.
- Before being considered as an IT standard, the requested IT must meet GSA's security and legal requirements using formal review processes.
- The GSA Standard Desktop Image, agency-wide Blanket Purchase Agreements, and other operational lists of technologies must align with the GSA IT Standards. Information technologies require a GSA- approved —terms of service agreement for use in GSA.
- GSA program managers and contracting officials are responsible for including language requiring a determination of compliance to the GSA IT Standards in appropriate goods and services acquisition documents. Information Technologies acquired through any means – including but not limited to formal contract vehicles, credit cards, or open-source – must comply with the GSA IT Standards. IT services that are externally provided, such as by third parties, must be interoperable with the GSA IT Standards.
- Only those Information Technologies listed as a GSA IT standard or fitting within the scope of a conditional-use approval are authorized for use; those not listed or not fitting within the scope of conditional use are subject to removal.

1.4.1 EARC Evaluation of Non-standard Software

The software evaluation process consists of legal and IT Security evaluation. The **Enterprise Architecture Committee**, (please note: the letter “R” does not stand for a word, it was placed in the abbreviation to distinguish it from another group called EAC) takes input from both legal and IT and makes a final decision on whether that software is approved for wider use at GSA. The EARC has representation from GSA IT Building and Energy Systems Team. During the review process, the software requester (you) may be contacted with additional business questions when needed. Typical questions include: "how many people will use the software", "What is the cost and is it recurring", and "whether any already approved alternatives were considered".

The software review process is kicked off by a catalogue request on [ServiceNow](#). Please be sure to keep your Building and Energy Systems Technical Project Manager included in the process so that they can ensure it goes through the appropriate reviews. Here's a link which shows [how to submit a software request](#).

For a software to be added to the "[GSA IT Standards Profile](#)" it has to **reviewed and approved by Legal, Security and EARC**. Please note: this is not an Approved Products List. This only lists the software that has gone through the review process and has been approved for use in the GSA environment. Once software has been permitted for use, the requester will be notified and it will be added to the GSA IT Standards Profile. The overall duration of the above process can take anywhere between ~2-6 weeks.

- **Legal Review of the End-User License Agreement (EULA)**

The End-User License Agreement (EULA) needs to be made available to GSA IT Building and Energy Systems Team **before** contract is signed for evaluation and acceptance. A soft copy of the embedded EULA needs to be emailed to the Building and Energy Systems team. The B&E Systems Team will then submit the EULA to be approved by the Office of General Counsel (OGC). The OGC reviews terms of service and determines whether or not any of the terms need to be modified or eliminated before the government can agree. Please see EULA fail chart and details in Chapter 5.

- **Security and Testing of Non-Standard Software**

- The software must adhere to the United States Government Configuration Baseline (USGCB) and be able to operate under a user context (i.e. does not need local admin rights to run).
- GSA IT will test the client software to ensure it integrates properly with the standard GSA image. Upon testing of the software by GSA IT, any requested changes to the software for compliance or compatibility reasons, must be made prior to acceptance.
- The length of this review process is dependent on the changes required in the EULA and changes (if any) to the software prior to installation.
- Projects need to ensure that only approved software is installed at their building which will ensure that it will work with the GSA image and pass security assessment. Local Support's ability to address client software issues on BSN Consoles (See BSN Section 1.7 below) will be limited and can almost never be provided remotely.

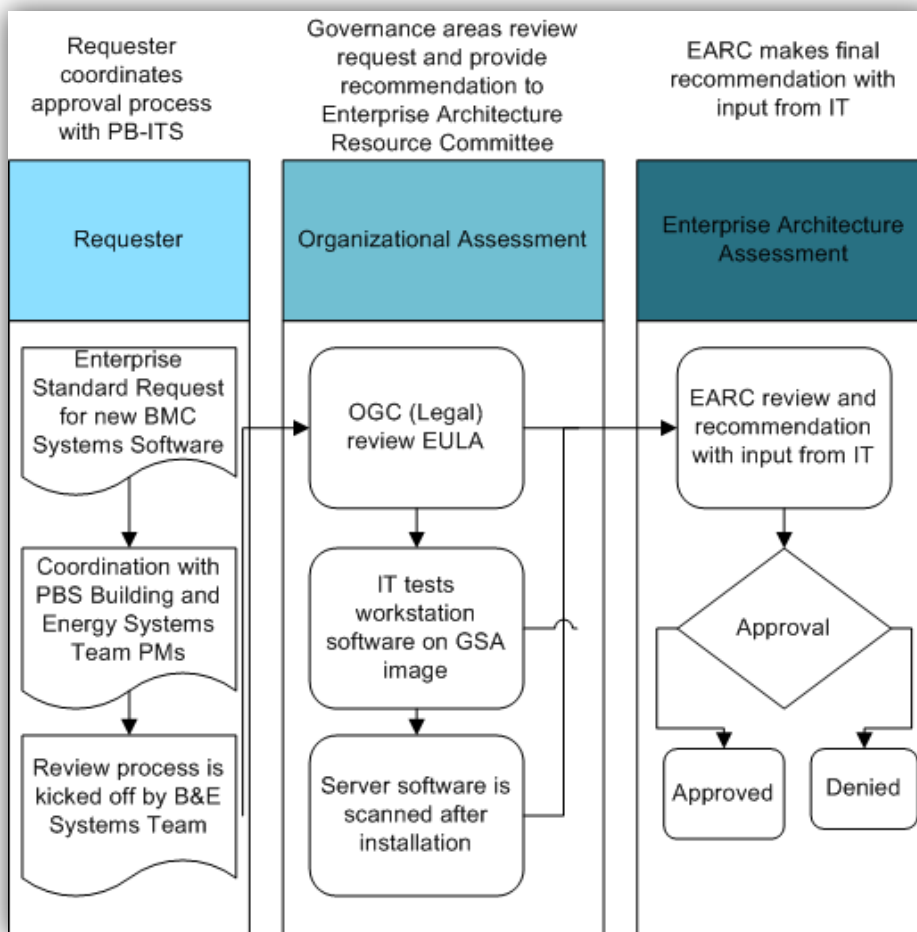


Figure 1-1: Nonstandard software Approval Process

1.4.2 Non-standard software on GSA workstations

If there is a need to install a non-standard software on a GSA workstation, discuss the application need with your [Building and Energy Systems Technical Project Manager](#). If the software has not yet gone through the EARC evaluation process, then it will need to be completed before the software is installed. If software *has* been previously approved, then the request for install can be initiated through a catalog request on [ServiceNow: Service Catalog > Equipment Requests > Software Requests > Software](#).

1.4.3 Non-standard software on GSA servers

The software approval process also applied to BMC server applications. The only difference is that servers are hardened before they are deployed and made available to the project.

1.5 Security Assessment and Evaluation Process for BMC Systems Devices

Information technology systems which will be placed in GSA buildings are required to be evaluated against GSA IT policy compliance requirements.

Systems unable to compensate to new issues discovered by the assessment process, risk suspension of their Authorization to Operate in the Federal Government. Please note: GSA IT highly recommends that contracts for products and services should include warranties

and support, therefore vendor would be responsible for any maintenance and support of their devices and language to this effect should be included in the contract.

1.5.1 GSA IT Security Scanning Process

In order to be used in a production environment, a scan must be complete, and vulnerabilities either remediated or have an Acceptance of Risk (AOR) by GSA IT's Authorizing Authority. Please note: scans are authenticated and have a process in place to securely pass authentication data.

There are two methods to get scans completed:

- In IT Security test lab or;
- On-site via GSA Site Remote Scanning.

• IT Security Test Lab Scan

In order to request a scan, the [Scan Request Form](#) located on Google Site must be completed, before the device is shipped to GSA IT Security to be scanned. The site is available to anyone with access to the GSA network. To access the scan request form, click the "Assessment Request Form" link. Scan request forms must be complete in order to be approved, and all relevant documentation (installation manual, configuration management plan, hardening guide) for the device should be supplied along with the form. At the end of the Scan Request, there is a link that instructs you to attach files to a shared Google folder. Please be sure to include the exact device name (as it appears in the scan form) to associate the documents with the scan request form.

The device should be sent to the GSA IT lab configured and hardened as it will be installed on the GSA network (unnecessary ports and services closed, etc). The device should also arrive properly assembled for power. The IT Security team is not permitted to work with any electrical wiring, and any device that cannot immediately be plugged into a 110V wall plug will be delayed (either returned for proper configuration, or on hold until someone can come to the lab and configure appropriately).

NOTE: Any configuration required by IT Security or lack of documentation may result in delaying the security evaluation process. If you have any questions regarding this process feel free to contact BMC.IT.Security@gsa.gov

The device should be shipped to the following address:

ATTN: Bernard Ellsworth
U.S. General Services Administration
GSA IT Security
1800 F Street NW, Seat (1475B)
Washington, DC 20405-0001

For more details on the assessment process, please visit [InSite](#).

• GSA Site Remote Scan

As with test lab scan, a Scan Request Form must be completed, in order to request a remote scan. Any relevant documentation should be submitted along with the form.

Project manager, the building manager or the regional GSA-IT manager must coordinate with the Network Operations (NetOps) team to ensure that a secure VLAN segment has been set up and identify the port to plug device(s) in for remote scanning by GSA IT Security team.

Coordination must be established between the site and the GSA IT Security team to provide the required testing and evaluation of any new device.

If you have any questions regarding this process feel free to contact

BMC.IT.Security@gsa.gov

NOTE: Test lab scans are always preferred over a remote scan, due to the additional logistical hurdles involved in coordinating remote scans.

- **Manual Assessment and Evaluation** Manual assessment of devices include , ensuring the device is:
 - Properly configured- services and configurations should be as it will be installed at the field site.
 - Properly constructed - fully assembled device as we do not complete any wiring of connections or have power supplies .
 - Properly documented- documentation such as device Installation manual, configuration Management Plan and Hardening Guide are sent or emailed to GSA IT before device is scanned.

If any of these items are missing, GSA IT will return the device without scanning it.

1.5.2 Security Assessment Report

Upon completion of the security review, a Security Assessment Report (SAR) is provided. The SAR includes the assessment results identifying potential security vulnerabilities. Vulnerabilities are categorized into risk levels (High, Moderate, or Low). The GSA IT Security team provides recommendations for correcting or mitigating the identified issues. The result of each scan will be provided as part of the final assessment report. The SAR is sent to the vendor, regional Point of Contact (POC) and any other stakeholder authorized to view the report. The GSA IT Security Team then updates the Device Evaluations status page on InSite (GSA's intranet) once a device which has been evaluated, with non-sensitive information.

1.5.3 Issues Identified During Security Evaluation

Issues identified from a security review must to be addressed by the vendor or appropriate service provider. The GSA IT Security team will provide guidance. Vulnerabilities should be mitigated by fixing the identified weakness or, if not possible to mitigate, the device/system owner must request that the Authorizing Official (AO) accept the risk the device/system would impose on the GSA network. Each vulnerability (High, Moderate or Low) must be mitigated Per GSA security policy, CIO P 2100.1. all High and Critical risk findings should be mitigated in 30 days and Moderate risk findings in 90 days. If remediation process goes beyond this time limit, then an Acceptance of Risk needs to be completed by the project and signed by the Authorizing Authority.

1.5.4 Post-Scan Follow Up

Once the SAR is sent, the IT Security team, in coordination with GSA IT and project POCs, will schedule a conference call to follow up with the vendor and/or designated POC to develop a plan of action to address the security findings. The vendor and/or POC is responsible for remediating vulnerabilities. If there are no fixes to resolve the vulnerabilities, or if the vendor fails to engage with GSA IT (within six months of assessment), then the device will be deemed as "non-remediated". Such devices are not acceptable on the GSA network. If a fix becomes available or if the vendor re-engages with GSA IT, for a non-remediated device, then it will need to go through the assessment process again.

Roles and Responsibilities

- **Building and Energy System Team's PM** – Communicates scanning requirements to the project team. Also coordinated scan kick off meeting between project team, vendor and GSA IT Security. This meeting is a chance for IT Security to understand a little more about the device and discuss process and expectations.

- **Regional POC** - This is the main POC of the project that will using the device in question. The POC must ensure Scan Request form is filled, proper documentation is included and device is properly configured and sent to IT Security. They will also be championing vendor engagement throughout the evaluation and remediation process.
- **GSA IT Security**- performs scan and communicates vulnerabilities to the stakeholders:
 - Ensures Scan Request Form is complete and accurate for devices scanned in IT Security Test lab and inform project team members of status or discrepancies.
 - For devices scanned at GSA site, ensures connectivity and account access to device once Regional POC confirms device is ready. Inform project team members of status or issues and work with regional GSA-IT or NetOps team to resolve.
 - Scan device upon successful connectivity and access.
 - Writes and send report to Vendor and Region POC (CC rest of Project Team) upon completed scans.
 - Follows up with Vendor and Region POC in order to review and implement remediation strategies
- **Vendor**
 - Provides POC to GSA IT Security
 - Provides device documentation to IT Security
 - Provides IT Security shipment tracking number (if device is sent)
 - Remediate device - engages with GSA IT and provides remediation documentation and strategies until GSA IT deems devices "remediated".

1.5.5 Building Technology Device Scanning and Vulnerability Remediation Process

- **Notification of Receipt and Acceptance for Induction** - The GSA IT Security Team will evaluate the device, documentation, scan request form, and any other required item to determine if it has what is necessary to perform a scan on the device. The device will then be inducted into the scanning process and proceed to the next defined step; or it will be rejected for scanning until the required items are provided. In those cases, the Acceptance for the induction phase will begin again
- **Induction and Scanning** – The GSA IT Security team will initiate and complete all required scans of the device.
- **Creation and Distribution of the Security Assessment Report (SAR)** – The GSA IT Security team will take the results of the scans and write a SAR. The SAR will clearly detail the specific security vulnerabilities associated with the device, and identify the level of risk associated with them. The SAR is considered sensitive and will be provided encrypted to the PBS Project Manager and the vendor/manufacturer point of contact associated with the integration and use of that device. A password for that report can be received by placing a

call to the GSA IT Security team.

- **Scheduling and Conducting a Review of the SAR with Stakeholders** – The GSA-IT Building and Energy Systems project manager, in coordination GSA IT Security will attempt to schedule a conference call with the PBS Project Manager and the appropriate vendor/manufacture points of contact to kick off the review process and work with the project team and vendor/manufacture to frame an agenda for the remediation of the vulnerabilities and/or risk associated with the scanned device. The remediation process is largely the responsibility of the vendor/manufacture and the PBS project manager. The GSA IT Security Team will provide guidance and assessment during the remediation process.
- **Response from the Vendor/Manufacturer** – We are recommending that the vendor/manufacture provide a response back to the GSA IT Security team and their PBS Project Manager, which details how they plan address each of the identified vulnerabilities and/or their associated risks, as well as a timetable for when that plan will be executed
- **GSA IT Security Follow-Up Response** – The GSA-IT Security team will review and provide feedback to the vendor/manufacture regarding their aforementioned response to the SAR and remediation work plan.
- **Successful Remediation of Identified Vulnerabilities** - The successful remediation of the vulnerabilities and their associated risks, which may be required for that device to be given approval to operate on the GSA network will be largely driven by the vendor's/manufacture's initiative and effort. The GSA IT Security team is committed to prompt responses to the vendor's/manufacture's inquiries and attempts to satisfy our Agency's IT Security policies.

1.6 GSA Network Access to Perform Duties

This section demonstrates how any GSA employee, contract staff or vendor/personnel can obtain access to GSA IT systems, which includes all hardware, system software, data and network access. Each of these requirements needs to be met in order for access to be granted.

1.6.1 HSPD-12 Credentialing and Systems Privileges

On August of 2004, President George W. Bush signed the Homeland Security Presidential Directive-12 (HSPD-12) which is a mandated a Policy a for a Common Identification Standard for Federal Employees and Contractors. HSPD-12 requires all federal Executive Agencies and departments to conduct personnel investigations, adjudicate results, and issue a Personal Identity Verification (PIV) or Access Card to all federal employees and contractors or personnel who require routine or regularly scheduled access to federally controlled facilities and information technology (IT) systems.

Please visit <http://www.gsa.gov/portal/category/26432> for details on how to initiate the credentialing process.

ENT domain credential and VPN access require HSPD-12 clearance. Please note: Regional Project Teams need to ensure Vendor personnel maintain their ENT accounts and keep them active, in order to be able to provide technical support going forward. This includes timely completion of all tasks required to keep an ENT account active, such as annual IT Security Training courses.

The mandatory minimum security clearance level for access to any GSA IT system is the preliminary adjudication of the National Agency Check with Written Inquiries (NACI);

however, the actual final clearance level needed is dependent on the security level of the data or systems being accessed by the individual. If the completed clearance process does not result in final favorable adjudication, previously granted provisional access will be revoked. The process to obtain this clearance can be found at insite.gsa.gov, Information Technology/Access Card Implementation/Policy and Guidance Resources. Personnel Security management is the responsibility of the requesting official.(Please see Appendix B for more information.)

Please note: per OMB mandate M-06-16 and GSA order CIO P 2181.1, “those individuals whose duties require a higher degree of trust, such as IT system administrators, those who handle financial transactions, or those who deal with PII, and other sensitive information (e.g., building drawings, etc.), will continue to require investigations associated with higher levels of trust such as the Minimum Background Investigation (MBI) or the Limited Background Investigation (LBI).” This means individuals who will need administrative access to BMC servers will need to have an MBI clearance.

Lastly, per GSA order 2100.1J, “authentication schemes for Moderate and High Impact systems must utilize multi-factor authentication using two or more types of identity credentials (e.g. passwords, SAML 2.0 biometrics, tokens, smart cards, one time passwords) as approved by the Authorizing Official and in accordance with the security requirements”. This means in order to gain elevated access to BMC systems, once MBI adjudication is completed, individuals will need to get a Shortname Account (SNA) and a token. Request for SNA and token can be submitted by the sponsor on [ServiceNow](#) > **Service Catalog** > **Account Services** > **New Account or Access Requests** > **GSA Short Name Account**

1.7 Building Systems Network (BSN)

As this chapter describes, there are Federal and GSA specific IT security policies and standards that apply to the purchase and/or use of any IT-related product or service. Any piece of hardware or software that does not meet these standards is thereby introducing a certain amount risk through the ownership and/or use of that system or component. Particularly those devices that are enabled for IP-based network communication are treated with the most caution, as they have the ability to impact and be impacted by other IP-based systems, which are the most prevalent types of systems associated with GSA's IT environment. Wireless based devices, or components with other capabilities deemed to introduce risk, are also subject to review by GSA's IT Security Operations and IT Security Engineering organizations.

The scanning and evaluation program outlined in this chapter is designed to identify potential vulnerabilities with any IP-based device that is being proposed for integration to the GSA network, to include the categorization of the risk associated with those vulnerabilities. Other non-IP based devices may require evaluation by GSA IT Security based on the capabilities of that device and any perceived risk it introduces. As defined in the scanning and evaluation process, the organized results of those scans are reviewed with the manufacturer or responsible vendor in an effort to have them remediate their devices so that the vulnerabilities either no longer exist or the risk associated with those vulnerabilities is either completely eliminated, or reduced to such a degree that the Authorizing Official is willing to accept that amount of risk and provide an Approval to Operate. An Authority to Operate is necessary for a system or component to have physical or logical access to the GSA network or to be used in GSA facilities.

The challenge associated with the various building technology systems is that while advances have been made in the core functionality of these devices necessary for making buildings easier to operate, that increased functionality, particularly as it relates to network communication, introduces increased risks. The advanced metering, building automation, lighting control and physical access control systems industries, for example, have not positioned themselves the way most other IT products companies have, with a focus on IT security. This gap in security is proving to be one that cannot be readily closed by companies

in these industries in a timeframe that is compatible with contractual substantially complete dates or other critical project deadlines. Still in other cases, where PBS sites are simply migrating their existing building systems to the GSA network, there is not a vendor with an open contract to engage in any of the improvements or risk mitigation related to their system components.

In an effort to meet the business requirements of our PBS customers, GSA IT developed a strategy and network security plan to allow these devices to be integrated in such a way as to substantially mitigate the risks associated with their use, both to the GSA business network (ENT domain) and the building systems themselves. This design will make use of a virtual network and access control lists (ACL) that will group the IP addresses associated with the building system devices, to include controllers, servers and user workstations, and restrict their communication from the rest of the GSA network. This concept is referred to as the Building Systems Network (BSN).

1.7.1 What is the Building Systems Network (BSN)?

The BSN is a strategy and design concept that leverages virtual networks and access control lists (ACL) to enable logical network segmentation between building systems and the GSA ENT domain, otherwise known as the GSA business network, both of which use the same physical network. The application of a private Class B network used for IP address assignment to building control system components, servers and workstations, facilitates the use of multiple ACLs to allow what is effectively “white listed” communication to GSA services required to enable IT support of GSA IT infrastructure within the BSN or to allow communications with approved external services for building systems.

1.7.2 Why is the BSN Necessary?

Over the past several years PBS-owned facilities have been making use of IP-enabled building control devices to support increased capability, ease of use, remote access and data integration. As the GSA IT Security team has concluded through their scanning and evaluation of these devices, the overwhelming majority of them have what are categorized as high risk or critical security vulnerabilities that are not permitted. Because the overwhelming percentage of building technologies has non-remediated vulnerabilities and introduces unacceptable risk to GSA, and because it will take significant amounts of time for these industries to evolve their products to meet federal IT guidelines, GSA has developed its own risk mitigation solution to insure that our facility managers and regional customers can continue to use this important technology for the lowest possible cost. The BSN is NOT intended as a replacement for the ongoing remediation of these devices by the vendors. All new products contracted for at GSA are required to meet the aforementioned NIST and FISMA standards to be given Authority to Operate in GSA facilities or on its network.

1.7.3 Who is Responsible for the Creation and Management of the BSN?

The BSN was designed with the participation of multiple groups within the GSA-IT, and with cooperation from subject matter experts in the regions.

- **The network management** portion of the BSN will remain the responsibility of GSA-IT's Network Operations team.
- **Citrix** will be managed and supported by the Citrix team and the PB-ITS Technical Operations team.
- **Workstation** configuration and support will be managed by regional GSA-IT

Local Support groups.

- **Server configuration** and support will be managed by the Technical Operations team.
- **Project management** will be the responsibility of the PB-ITS Building and Energy Systems team.

1.7.4 BSN Implementation

As of August 31st 2012, any building monitoring and control system in any region that requires access to GSA's network will be integrated onto the BSN, not the ENT domain, as was the previous practice. In October of 2012, we began the process to migrate those systems that currently reside on the ENT domain over to the GSA network.

1.7.5 What Changes Can Be Expected Once the BSN ACL is Applied

The advantage of the BSN design is that it makes use of all the existing physical infrastructure currently supporting building systems, eliminating system level changes, and requiring no expenditure or level of effort to effect this change. What will change is how the systems users will access the application(s) and the IP-enabled devices from a GSA workstation. Any multi-user workstation that resides on the GSA ENT domain, as all currently do, will no longer have direct access to these building control applications or IP-enabled devices. Instead, Citrix is the gateway to allow access from the ENT domain.

Because we recognize that in some rare situations Citrix may not be available or optimal, and that in the event your site's network connectivity to the GSA WAN is interrupted you will need to have control over your building systems, we will configure one or more of the GSA workstations provided to you to allow them to directly access the system application(s) and IP-enabled devices. This workstation(s) is referred to as the "Building Console", and it is not associated with the ENT domain, like a normal user workstation. The sole purpose and capability of the Building Console workstation is to provide direct access to the application and IP-enabled building system controllers. Because the workstation is statically addressed with a private IP from the field sites Energy Management Systems (EMS) subnet, it can only work if it is attached to the Local Area Network (LAN) at the field site it was intended for. Therefore, laptops configured as building consoles will not be usable from remote locations, and will not be granted VPN access.

All remote access to building monitoring control applications, once on the BSN, is only possible through Citrix, which is available on almost any type of personal computer or laptop. By design, there will not be any supported way to remotely access the vendor provided IP-enabled system devices.

1.7.6 Will the BSN Be Implemented the Same Way for Every Site?

Essentially, the implementation of the BSN is the same for each site. The only conceptual difference is how the ACLs are applied, which varies depending on whether a site is using physical or virtual servers or in some cases both. The following graphics illustrates those differences and describe the.

- **BSN Physical Server Scenario**

In this scenario, the physical server, which resides within the buildings BMC IP network, is segmented from the ENT. GSA ENT users are able to access the physical BMC server either through the Building Console workstation from within the building or through Citrix.

The advance meters themselves are segmented from the ENT, however, the BSN

Access List allows them to communicate to the ION Enterprise server. GSA ENT users are able to access ION EEM or the ION Enterprise server from their ENT workstation. Building Console workstation users can only access their building controls application server(s) from the building console. Neither ION EEM or the ION Enterprise servers can be accessed from a Building Console workstation.

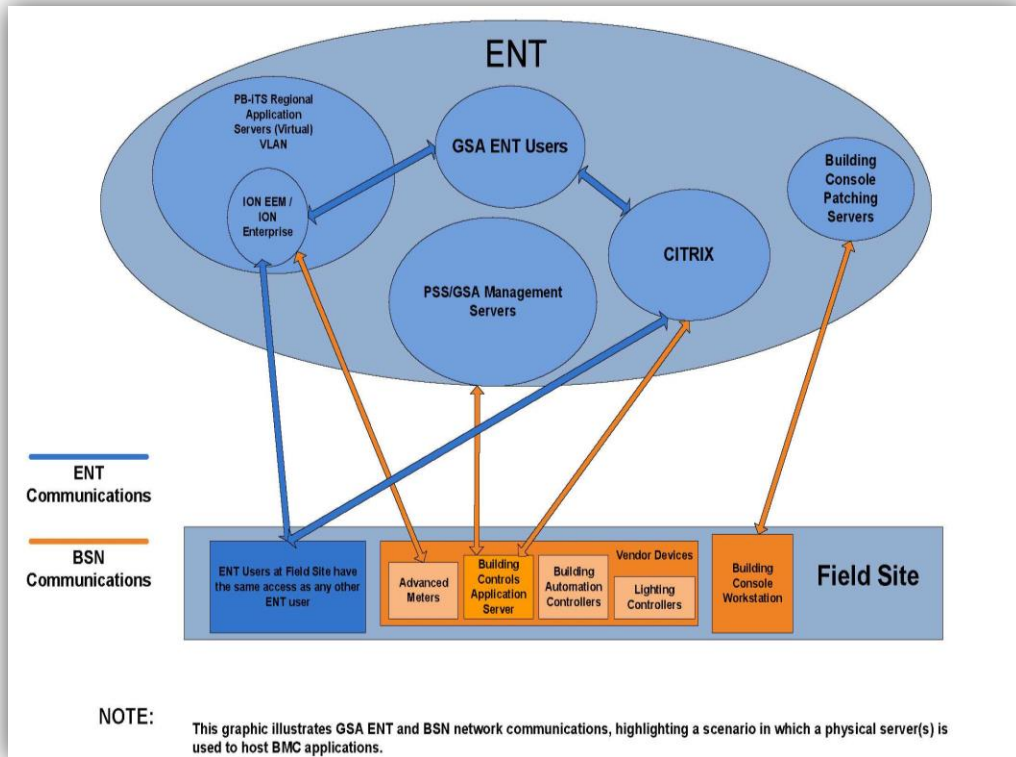


Figure 1-2: BSN Physical Server Scenario

- **BSN Virtual Server Scenario**

In this scenario, the virtual servers are built on a VLAN dedicated to the BSN virtual servers. The BMC controllers are segmented from the ENT, however, the BSN Access List allows them to communicate to the BMC virtual server. GSA ENT users are able to access the BMC virtual server either through the Building Console workstation, from within the building or through Citrix.

The advance meters themselves are segmented from the ENT, however, the BSN Access List allows them to communicate to the ION Enterprise server. GSA ENT users are able to access ION EEM or the ION Enterprise server from their ENT workstation. Neither ION EEM nor the ION Enterprise servers can be accessed from a Building Console workstation.

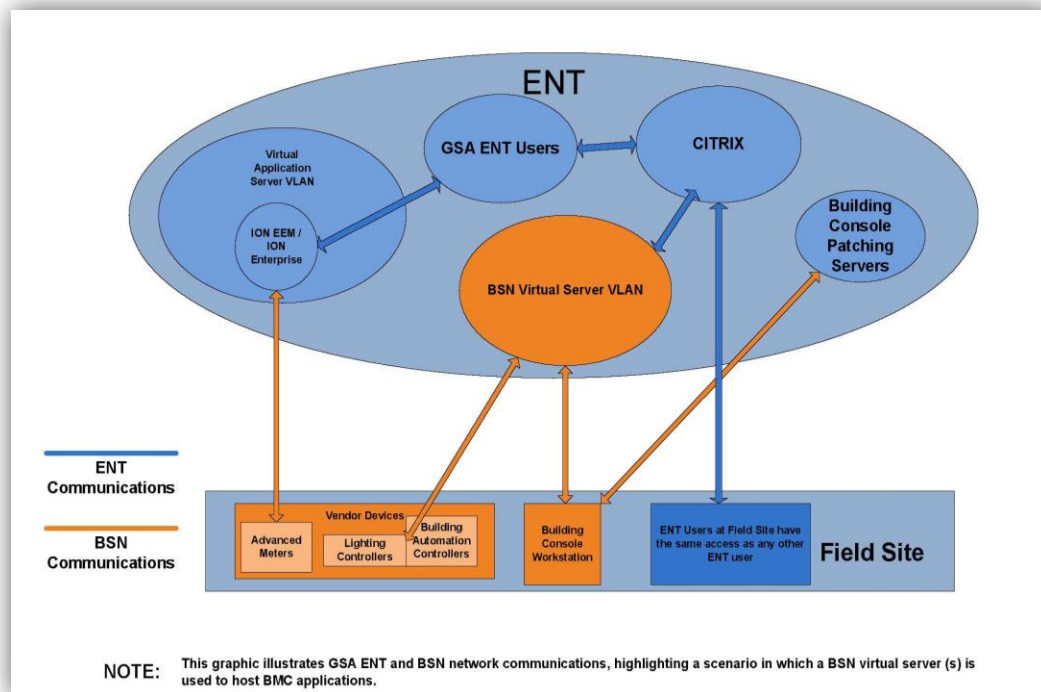


Figure 1-3: Virtual Server Scenario

1.7.7 BSN Building Consoles

BSN Building Consoles are GSA workstations (desktops or laptops) that receive a standard GSA image, but are not joined to the ENT domain the way normal GSA user workstations are. This means that they do not receive the same group policies, and do not adhere to the same IT security standards that a user's ENT workstation does. It also means that Building Consoles cannot communicate or interface with any sites or services that are available or that are made available by the ENT domain. This includes, but is not limited to GSA email, GSA.gov, the public internet, etc. The only thing that the Building Console can communicate to are building system application servers, and building system IP-based controllers, if those devices have a web or RDP interface. The Building Console and its communication restrictions are illustrated in the figures above.

- **Logging into the Building Console**

The building consoles have two local accounts that can be used to log in to the workstation. BSNuser is intended to be the primary account used by most users of the building console. The BSNadmin is the other account, which has full administrative rights to the workstation. GSA IT will manage the GSAadmin account and administrator privileges. Its sole intended use is for the purpose of adding or removing software from the building console.

- **Installing Software on the Building Console**

Any software that gets installed on any GSA computer hardware, including a Building Console must have the End User License Agreement (EULA) for that software approved by GSA's Office of General Counsel. To determine if a particular software product has already had its EULA approved, email pbs.pbios@gsa.gov and request confirmation. If it has not, the EULA should be provided to the same email address with a request for approval. PLEASE NOTE: unapproved EULAs will require revision from the manufacturer until the terms are acceptable to GSA and this process can be lengthy, and in some cases no agreement may be reached between GSA and the manufacturer.

While there is not currently a requirement that software be scanned by GSA IT Security before being installed on a building console, it is recommended that only approved software be used to insure that the software is compatible with GSA's image.

- **IT Support for Building Consoles**

The Tech Ops team provides front line support and management for all ticketed support requests from BMC users.

- User submits a ticket to IT Service Help Desk, ticket is routed to the Tech Ops team.
- Tech Ops team assesses that the trouble is related to a multi-user workstation issue and creates a separate ticket for that Region's Local Support.
- Local Support is understood to not have any remote utilities to troubleshoot the user workstation directly. The best level effort will include the following:
- Local Support will contact the affected user and provide telephone support to the end user to determine if the trouble can be corrected with guidance from local support staff.
- If the trouble cannot be resolved in aforementioned approach, the building console workstation will need to be shipped to the Local Support office
- Local Support will re-image the building console workstation, configure the same static IP and local accounts, and return to the end affected end user.
- Local Support communicates to the Tech Ops team if the building console workstation issue has been resolved, or if additional support from another IT service group is required.
- Tech Ops team closes the original ticket if the issues if resolved, or pursues troubleshooting operation and assistance from the appropriate GSA IT support group.
- PB-ITS is attempting to make one desktop and one laptop available in each region for break/fix issues, if repairs are expected to take a significant amount of time.

1.7.8 Using Citrix and Building Console Workstations

By using Citrix as the gateway for ENT-based and/or remote system access, the BSN will actually make remote access simpler and more readily available. While ENT credentials are still required, no longer will vendors need a GSA laptop with VPN access to log in to a server. They will be able to launch RDP sessions, or access published web apps (if available) right from Citrix, which will save them time and hopefully save the regions money. When vendors are on site they can make use of the Building Console workstation to access system applications and devices. For details on accessing Citrix, please see chapter 4.

The integration process to BSN is almost completely transparent to the field site, as all of the unique configurations are handled by the aforementioned GSA IT groups and the impact of this segmentation is completely transparent to the way these systems function, as it will be installed in the same manner as prescribed in the rest of this reference guide. The only variation to what some users currently experience is that because this virtual network will be segmented from the ENT or GSA business network, they will not be able to access their system or application directly from their GSA user workstation.

Instead they will have two options for access. Each site will be provided with a government furnished desktop and/or laptop, referred to as a Building Console Workstation, which will receive an IP address that is part of the EMS subnet and virtual network where the building system(s) resides. This workstation will not have access to the public internet or any other GSA application, such as email. For those GSA users who must use their standard GSA workstation they will be able to access their building systems through a gateway solution, most likely Citrix. The building system applications, whether web-based or client software based, will be available through Citrix and will function the same as if they were accessed directly with the only added step of logging into Citrix and then accessing the available link.

1.7.9 Steps to Integrate Sites on to the BSN from the ENT Domain

- **Citrix Access:** Publish applications and RDP links, building management staff test Citrix access.
- **Kickoff Meeting:** Discuss the tasks necessary for migration, roles and responsibilities, set migration date.
- **Preparation:** Accomplish pre-migration tasks.
- **Migration:** Conference call with GSA IT groups and building management staff, execute migration tasks, test, site acceptance.

1.8 Incident Response and Disaster Recovery

1.8.1 Incident Response

Per CIO-IT Security-01-02 Rev 12, an information security incident can be thought of as imminent threat/violation of information security or privacy policies. Be mindful and suspicious of unusual activities when it comes to your BMC systems. Cyber-attacks, malware and viruses can cripple your system and impact the GSA network. If you notice any suspicious activity, contact the GSA IT Service Desk at [866-450-5250](tel:866-450-5250) or ITServiceDesk@gsa.gov, and the GSA Incident Response Team will investigate the issue.

1.8.2 Disaster Recovery

Since building monitoring and control systems that reside on the GSA network rely on IP network communications and computer hardware, they are subject to the impacts associated with interruptions in service of that IT infrastructure. In order to prepare your facility's BMC system in the event of a data circuit failure, Local Area Network (LAN) outage, cyber-attack or application server failure, Disaster Recovery (DR) preparations need to be planned and tested. An effectively developed Disaster Recovery (DR) Plan will ensure that while network communications may be temporarily unavailable, building control system components will continue to function, and in fact may also be programmable if local software based tools are available, ensuring that building operations will not be significantly impacted. **This means the BMC contractor will need to document and submit operational procedures to monitor and control systems in case of an outage, to ensure continuity of operations, as part of the commissioning process.** Once the plan is developed a Disaster Recovery (DR) exercise will simulate an IT outage limiting the IP based controllers ability to communicate to the application server and/or to other parts of the network. Executing the DR exercise will require coordination and participation from Regional Managers, Property Management, Operations and Maintenance and GSA IT. Please work with your Building and Energy Systems PM to schedule a Disaster Recovery (DR) exercise.

Appendix A: Contact Information

Item	Contact information
GSA IT Security	BMC.IT.Security@gsa.gov
PBS Application Support Team	pbsapps.support@gsa.gov
Building and Energy Systems Team	pbs.pbios@gsa.gov B&E Google Site
HSPD-12 credentialing questions	accesscard@gsa.gov hspd12.pmo@gsa.gov

Appendix B: Listing of Reference Policies

Item	Guide/Document Name	Description
B.1	FIPS 140-2	Federal Information Processing Standard (FIPS) is a certification that specifies the exact module name, hardware, software, firmware, and/or applet version numbers. Encryption is an important tool used to meet security control requirements. When used to protect sensitive information Federal systems must use encryption that meets the requirements of the Federal Information Processing Standard (FIPS) 140-2. Once a system has been designed and deployed using FIPS compliant technologies it must be operated following documented procedures to ensure keys are created, stored, retired, revoked and otherwise managed in a consistent and secure manner. The National Institute of Standards and Technology (NIST) promulgated FIPS 140-2 to ensure that encryption technology meets minimum standards when protecting sensitive data on Federal networks and systems. All cryptographic modules used in Federal systems must meet the standards in FIPS 140-2. FIPS 140-2 provides a certification path for vendors of cryptographic modules. Certification ensures that the standards are met in the specific vendor implementation. Wireless and SFTP (Secure File Transfer Protocol) Data Transmissions also need to meet FIPS 140-2 protocol. (See FIPS 140-2 http://insite.gsa.gov/graphics/staffoffices/keymgmt.doc)
B.2	IT Security Procedural Guide: Key Management CIO-IT Security-09-43	http://insite.gsa.gov/graphics/staffoffices/keymgmt.doc
B.3	GSA Order CIO 2100.2B GSA Wireless Local Area Network (LAN)	https://insite.gsa.gov/portal/content/636958

	Security	
B.4	4 Federal Desktop Core Configuration (FDCC) standards Checklist	http://web.nvd.nist.gov/view/ncp/repository
B.5	GSA HSPD-12 Personal Identity Verification and Credentialing Handbook	http://insite.gsa.gov/graphics/staffoffices/HSPD12_Handbook_v8.pdf
B.6	GSA order CIO P 2181.1" - see page 25: Homeland Security Presidential Directive-12 Personal Identity Verification and Credentialing	https://insite.gsa.gov/portal/getMediaData?mediaId=681066
B.7	GSA order 2100.1J GSA Information Technology (IT) Security Policy	https://insite.gsa.gov/portal/mediaId/513044/fileName/GSA_Information_Technology_(IT)_Security_Policy_CIO_21001J___12-22-2015.action
B.8	OMB M-06-16 Protection of Sensitive Agency Information	https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m06-16.pdf
B.9	Access Card Policy and Guidance Resources	http://www.gsa.gov/portal/category/26432
B.10	2100.1I CIO P GSA Information Technology (IT) Security Policy	https://insite.gsa.gov/portal/content/610750
B.11	CIO 2160.1D GSA IT Standards Profile Policy v8	https://gsa.my.salesforce.com/06930000002OvWb
B.12	NIST 800-82 rev 2	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

B.13	NIST Special Publication 800-137	http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf
B.14	Contingency Plan [CP] [CIO-IT-Security 06-29,Rev 2]	https://insite.gsa.gov/portal/getMediaData?mediaId=672134
B.15	Continuous Monitoring Strategy Program [CIO IT Security 12-66]	https://insite.gsa.gov/portal/getMediaData?mediaId=691230
B.16	Managing Enterprise Risk: Security Assessment and Authorization, Planning and Risk Assessment [CA, PL &RA] [CIO IT Security 06-30, Rev. 8]	https://insite.gsa.gov/portal/getMediaData?mediaId=672866
B.17	CIO 2160.1D GSA IT Standards Policy v8	https://gsa.my.salesforce.com/06930000002OvWb
B.18	OMB M-06-16	https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m06-16.pdf
B.19	Incident Response CIO-IT Security-01-02 Rev 12	https://insite.gsa.gov/portal/getMediaData?mediaId=515961

Appendix C: Security for GSA Building Automation Systems

All GSA IT systems must be in compliance with the latest version of GSA's IT Security Policy (CIO P 2100.1). This includes building automation, advanced metering, and physical access control systems.

GSA IT Security Evaluation Schedule

All BMC systems devices that will be used on the GSA network must be evaluated by the GSA IT Security team. The evaluation process consists of security scans (operating system, web interface [if applicable], and database [if applicable]), a manual evaluation, and the writing of a security assessment report (SAR), and the process can take, on average, 25 business days.

Common Security Vulnerabilities

- Most common security vulnerabilities seen in BMC systems devices:
- Insufficient Documentation
- No Configuration Management Plan
- No Encryption / Weak Encryption (for sensitive data and/or login credentials)
- Unnecessary Services Enabled (FTP, Telnet, etc.)
- Unnecessary Ports Open
- Cross-Site Scripting Vulnerabilities
- Least Privilege Not Enforced
- Insufficient Auditing

Specific Security Requirements for GSA Building Automation Systems

All BMC systems devices that will be implemented on the GSA network must meet the following requirements:

1. All relevant information and documentation must be provided to PBS IT Security, including:
 - a. Firmware and software versions (these are essential for determining a security baseline)
 - b. Technical specifications (including information on all inbound and outbound communication on the device, required ports and services, etc.)
 - c. User manual
 - d. Installation and configuration guide
2. The device and software documentation must provide information to the System configuration management plan, explaining:
 - a. How will the device be configured on the GSA network, and how can this configuration be monitored?
 - b. How will the device be hardened (which ports and services are unnecessary and will be turned off when installed on the GSA network)
 - i. All unnecessary ports must be closed
 - ii. All unnecessary services must be disabled
 - c. How will the device be upgraded / patched when updates to firmware or software are released?
3. The device must have sufficient access controls, including:
 - a. Login screen
 - b. Password field on login screen must be masked
 - c. Passwords must meet GSA policy strength requirements: a minimum of eight (8) characters and must contain a combination of letters, numbers, and special characters
 - d. Logins must be encrypted (see #5 below)
4. The device must be capable of managing user access rights:
 - a. Least privilege – nobody should have more rights than needed (i.e., a user with a need for read-only / monitoring access should not be able to make changes to the device or the things controlled by the device)
 - b. Documentation (see #1 above) should state how user access rights are managed: administrators, general users, etc.
5. The device must be capable of utilizing TLS (SSL is not sufficient) for the

- encryption of sensitive data and/or login credentials
 - a. Project PM must state what kind of data is being transmitted through these devices (Metering data? Energy use data? Is the data sensitive?)
 - b. All web-based logins must utilize TLS
- 6. The device must be capable of logging the following auditable events:
 - a. Successful and unsuccessful account logon events
 - b. Account management events (creation or deletion of user accounts, change in user privileges, etc.)
 - c. Privilege use events (e.g., administrator functions, changes to or erasure of system logs, etc.)
 - d. System events (e.g., power failures, lost connection to a server, or other availability issues, system time changes, NTP server synchronizations, etc.)
- 7. If the device has a web application, the web application must be capable of logging the following auditable events:
 - a. All administrator activity
 - b. Authentication checks (e.g., user logons)
 - c. Authorization checks (e.g., checks of user privileges or access rights)
 - d. Permission changes (e.g., change in user privileges)
- 8. The device must be capable of being updated:
 - a. To address code vulnerabilities in the firmware
 - b. To improve the software or firmware in general (NOTE that major firmware revisions may require reassessment and reauthorization of the device.)
- 9. If the device uses a Microsoft Windows (except Windows CE) or UNIX/Linux based operating system, antivirus software must be installed and a plan must be in place for keeping the AV software updated
- 10. All new contracts with building automation system vendors should include support language to ensure that security requirements / upgrades will be met by vendor or manufacturer at no additional cost to GSA

Appendix D: Top Ten Most Common Vulnerabilities in BMC Systems Scans

Finding:	Cross-Site Scripting		
Finding Description:	This could result in impacts such as a hijacked account, information theft, browser redirection or denial of service.		
Host IP Address:		Scan/Script Risk Level:	Critical

Recommended Fix:	Cross-Site Scripting attacks can be avoided by carefully validating all input, and properly encoding all output. Implement validation globally using standard ASP.NET Validation controls, or directly in your code. More information: http://www.owasp.org/index.php/Top_10_2010-A2		
-------------------------	--	--	--

Finding:	Insufficient Documentation		
Finding Description:	The documentation available for the device does not provide administration instructions or complete information on the inbound and outbound communications of the device.		
GSA Guide or 800-53 Reference:	SA-5	Risk Level:	High
Recommended Fix:	GSA CIO 2100.1J requires that, "Documentation must be obtained or created to describe how security mechanisms are implemented and configured within the IT system." Obtain documentation sufficient to install, configure, administer, and monitor these devices.		

Finding:	Least Privilege		
Finding Description:	The documentation available for the device does not provide required configuration settings to enforce least privilege compliance.		
GSA Guide or 800-53 Reference:	AC-6, CM-2, CM-6	Risk Level:	High
Recommended Fix:	GSA CIO 2100.1J requires that, "Information systems must be configured to the most restrictive mode consistent with operational requirements and in accordance with appropriate procedural guides from NIST and/or GSA to the greatest extent possible. Implemented configuration settings should be documented and enforced in all subsystems of the information system." Obtain documentation sufficient to securely configure these devices.		

Finding:	Configuration Management		
Finding Description:	The documentation available for the device does not provide a		

	configuration management plan.		
GSA Guide or 800-53 Reference:	CM-2, CM-3, CM-6	Risk Level:	High
Recommended Fix:	GSA CIO 2100.1J requires that, "A system configuration management plan must be developed, implemented, and maintained for every IT system managed by GSA." Document and implement a configuration management plan to ensure that changes are authorized, tracked and validated.		

Finding:	Insufficient Auditing		
Finding Description:	No evidence was provided that the device is auditing to GSA required level of detail.		
GSA Guide or 800-53 Reference:	AU-2	Risk Level:	High
Recommended Fix:	Document, add, and enable auditing features to the devices. GSA CIO P 2100.1J states, "Security-activity auditing capabilities must be employed on all GSA information systems using GSA CIO IT Security 01-08, 'Auditing & Monitoring Guide'		

	and NIST SP 800-37 as guides.” Ensure that audit logs are in compliance with GSA auditing requirements.		
--	---	--	--

Finding:	Unencrypted Login Form		
Finding Description:	An attacker who exploited this design vulnerability would be able to utilize the information to escalate their method of attack, possibly leading to impersonation of a legitimate user, the theft of proprietary data, or execution of actions not intended by the application developers.		
GSA Guide or 800-53 Reference:	IA-5, IA-7, SC-8, SC-9, SC-13, SC-23	Risk Level:	High
Recommended Fix:	Ensure that sensitive areas of your web application have proper encryption protocols in place to prevent login information and other data that could be helpful to an attacker from being intercepted. GSA CIO P 2100.1J states, “Web sites (internal and public) with logon functions, must implement TLS encryption with a FIPS 140-2 validated encryption module.”		

Finding:	Logins Sent Over Unencrypted Connection		
Finding Description:	An attacker who exploited this design vulnerability would be able to utilize the information to escalate their method of attack, possibly leading to impersonation of a legitimate user, the theft of proprietary data, or execution of actions not intended by the application developers.		
GSA Guide or 800-53 Reference:	IA-5, IA-7, SC-8, SC-9, SC-13, SC-23	Scan/Script Risk Level:	High
Recommended Fix:	Ensure that sensitive areas of your web application have proper encryption protocols in place to prevent login information and other data that could be helpful to an attacker from being intercepted. GSA CIO P 2100.1J states, "Web sites (internal and public) with logon functions, must implement TLS encryption with a FIPS 140-2 validated encryption module."		

Finding:	No Encryption		
Finding Description:	Sensitive information is transmitted without protection.		

GSA Guide or 800-53 Reference:	IA-5, IA-7, SC-8, SC-9, SC-13, SC-23	Risk Level:	High
Recommended Fix:	Ensure that sensitive areas of your web application have proper encryption protocols in place to prevent login information and other data that could be helpful to an attacker from being intercepted. GSA CIO P2100.1 states, "Web sites (internal and public) with logon functions, must implement TLS encryption with a FIPS 140-2 validated encryption module". Sensitive information, including usernames and passwords, could be intercepted.		

Finding:	Unnecessary Services		
Finding Description:	Services were available with no documented need for their use.		
GSA Guide or 800-53 Reference:	CM-7	Risk Level:	Medium
Recommended Fix:	Disable all unnecessary services. Document all necessary services. Unnecessary services provide malicious user additional vectors to perform an attack.		

Finding:	Unnecessary Ports Open		
Finding Description:	Ports were open with no documented need for their use.		
GSA Guide or 800-53 Reference:	CM-7	Risk Level:	Medium
Recommended Fix:	Close all unnecessary ports. Document all necessary ports. Unnecessary ports provide malicious user additional vectors to perform an attack.		

Chapter 2

Network Infrastructure

2.0 Overview

This chapter will focus on networking protocols, specifically TCP/IP, used to form an inter-building network and BACnet, a data communication protocol for building automation and control networks.

A network can be defined as a collection of interconnected devices that facilitate communication among a set of users or devices, allowing them to share hardware, software, resources and information. Networks use a variety of protocols to organize and communicate data amongst the devices connected to that network. Primarily, an Ethernet based network, which supports the TCP/IP protocol, is used to form an inter-building or site network. This is the case for GSA and the vast majority of commercial and residential network services. Other intra-building networks, used to connect components, devices or appliances, associated with a specific system(s), such as building automation or lighting systems, use other protocols to communicate amongst the interconnected components. Wired technologies include Cat5e/Cat6 cables, as well as optical fiber cable. There are two main geographically based configurations for Ethernet networks. A Local Area Network (LAN) is a network that connects computers and devices in a limited geographical area such as an office building, or closely positioned group of buildings. Whereas, a Wide Area Network (WAN) covers a large geographical area such as a city, or country. A LAN has a higher rate of data transfer, 100/1000 Megabits per second (mps). GSA's WAN connects regional offices and headquarters. WAN connection speeds vary greatly and are determined by multiple factors. Please see chapter 1, section 1 for roles and responsibilities regarding GSA LAN/WAN.

The following illustration (figure 2-1) is GSA's Multi-Protocol Label Switching (MPLS) backbone. It shows the internetworking between GSA's Regional Office Buildings (ROB).

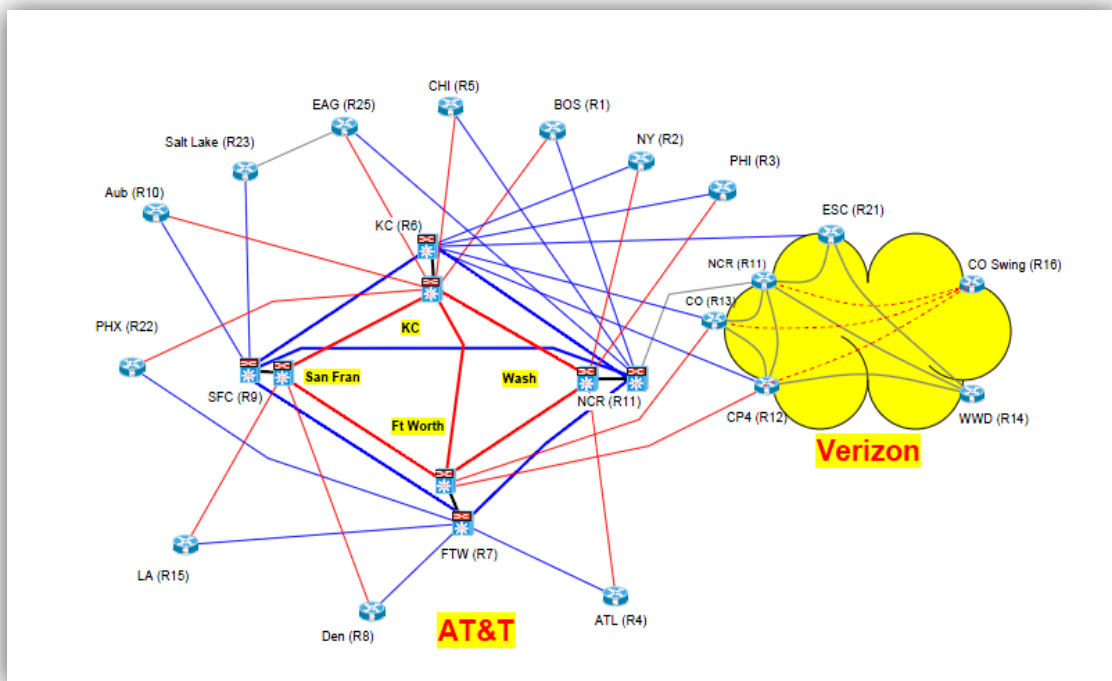


Figure 2-1: GSA MPLS Logical Backbone

The GSA WAN component is based on a combination fiber-optic premise cabling system and Cisco router-based technology. GSA WAN is located at all the Regional Office buildings (ROB's) and in the main data centers across the country. It is also the focal point for GSA's Internet access, which includes four MPLS (6-G (500 Mbps), 7-G (500 Mbps), 11-G (1000 Mbps), 13-G (1000 Mbps)) links to the Internet Service Provider (ISP) that are totally independent and provide for redundancy. The core backbone network is made up of Cisco routers and layer 3 Cisco Switches.

This chapter will define acceptable network topologies, standards for interconnection with the GSA network and the process by which network designs will be approved.

2.1 Roles and Responsibilities

2.1.1 PB-ITS Building and Energy Systems Technical Project Manager

Responsible for all Information Technology Systems within the Public Buildings Service and facilitates, including the review and approval of network design diagrams with the NetOps team. Your Building and Energy (B&E) Systems Technical Project Manager (PM) is the main point of contact, coordinating all activities between project managers and the Network Operations (NetOps) team.

2.1.2 GSA-IT's Network Operations (NetOps) Team

Manages the wide and local area networks (GSA WAN and LAN) and provides network security management for GSA infrastructure to include firewalls, intrusion detections and virus detection systems:

- Has the responsibility for the entire IP transport layer to include all routing and switching equipment and access to IP connectivity
- Has command responsibility for the GSA Local Area Network (LAN) and GSA Wide

Area Network (WAN) and is the sole provider for any and all IP addresses for devices associated with its network. NetOps also responds to network access and issues relating to IP connectivity

2.2 Standards for Interoperability

The following is a high-level list of items to consider for the implementation of an appropriate network design. **Please note:** hardware will not be deployed on the GSA network unless a network diagram is submitted by the project team and is reviewed and approved by NetOps. Diagram reviews and feedback are coordinated through the PBS Building and Energy (B&E) Systems team.

- GSA-IT NetOps, will support the entire IP transport layer from the point of network access, (i.e. GSA router) all the way to the point of demarcation, which is conceptually defined as the connection point to the vendor provided gateway (IP addressable) device(s). This gateway on the aforementioned IP network is the gateway to the secondary protocol network, which supports the vendor-provided building system devices and components. Please note: secondary protocol could also be IP-based. Further direction on the support of this solution will be provided in future iterations of the Reference Guide.
- Prior to release of a statement of work (SOW), issuance of a Request for Proposal (RFP) and/or a contract, a proposed network diagram needs to be submitted to PB-ITS B&E Systems team to be reviewed with all concerned parties. Feedback on the network diagram will be provided within 10 business days of submittal.
- Devices should **not** be plugged directly into workstations or servers.
- Data collection should **only** be done on systems classified and operated as servers and not workstations.
- All wireless devices must be pre-approved prior to contract award. FIPS 140-2 is required for all wireless communication devices. (FIPS 140-2 specifies 256 bit AES encryption)
- All switching and routing hardware will be provided, managed and maintained by NetOps.
- Vendor-provided media converters, hubs, switches and routers will **not** be accepted.
- Where possible, the same network gear is leveraged to support all approved agency hardware, including but not limited to user workstations and BMC devices.
- No intermediary devices are allowed on the GSA network. Switches provided by NetOps are configured to detect and disengage with such devices on the network.
- All IP-enabled devices, prior to deployment, will be subject to scanning and certification.
 - o For details on the scanning process, please see Chapter 1
 - o All devices on the GSA network are subject to continuous monitoring and periodic scanning by GSA-IT.
- If additional switches are required specifically to accommodate another project, an existing switch will be leveraged to accommodate the project.
- Switches should be connected using the uplink port only.
- Only GSA furnished computer hardware is permissible (desktop, laptop, server and peripherals).

- Only GSA furnished network equipment is permissible (routing and switching).
- All IP enabled devices must connect to the GSA switch.
- All IP addresses will be provided by NetOps, in coordination with the PB-ITS Building and Energy Systems Technical Project Manager.
- Subnets cannot be provided before the quantity of IPs and switchboards are specified.
- For new installations, PB-ITS prefers the local vendor to complete the cabling for all IP-enabled devices back to the GSA-provided switches, in accordance with the GSA Telecommunications Distribution Design Guide (TDDG). Once the cabling is completed and approved, support for the cable will become the responsibility of the GSA IT Local Support team. For existing systems, PB-ITS encourages the project team to work with the vendor to complete as much cabling as possible.
- In order to migrate an existing cabling infrastructure to a GSA-approved system, cabling may need to be reworked. In the cases where existing contracts with the vendors have expired, Regions can work with PBS-ITS and Regional GSA-IT Support to complete this cabling. Depending on the extent of the cabling job, arrangements for the cabling may vary. Please note regional IT support for cabling may not always be feasible or available.
- Network diagram must be reviewed and approved by GSA-IT NetOps before hardware can be configured and sent to the site.
- For existing implementations (retrofit) the project team needs to ensure that any non-standard switches and router are replaced by GSA standard switches and routers provided by GSA-IT NetOps.
- All IP-based traffic, will be issued, managed and maintained by NetOps.
- All contractors who require access to GSA hardware, network and/or systems, must become a credentialed GSA user on the ENT domain. Preliminary adjudication of the National Agency Check with Written Inquiries (NACI) clearance is a mandatory prerequisite for this access. No data will be transmitted outside the GSA network without government approval. Regional Project Teams need to ensure Vendor personnel maintain their ENT accounts and keep them active, in order to be able to provide technical support going forward. This includes timely completion of all tasks required to keep an ENT account active, such as annual IT Security Training courses.
- All Ethernet (IP-enabled) devices need to terminate at a GSA switch.

2.3 Network Topology

The following (figure 2-2) is not intended as a network diagram, but rather a topology that demonstrates the types of logical interconnections amongst vendor provided devices and the GSA LAN and WAN. This demonstrated logic should form the basis in approach for the design of an integrated building controls and/or energy system.

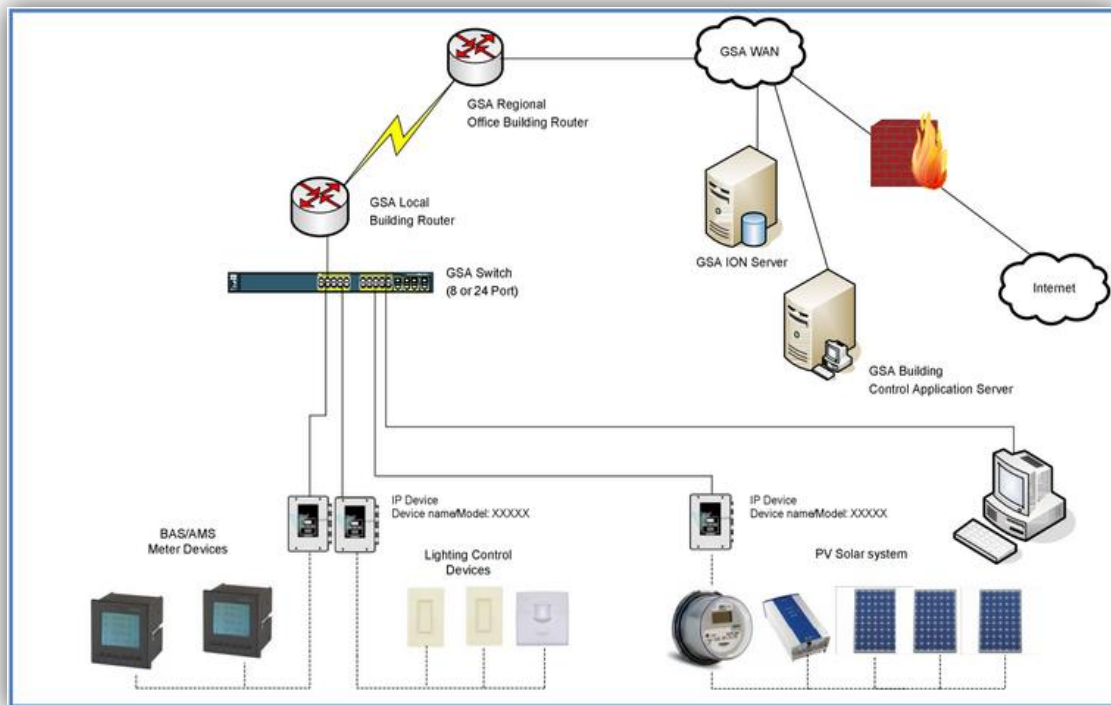


Figure 2-2: Sample Network Topology

2.3.1 Network Design Requirements: Submitting a Network Design Diagram to PB-ITS and NetOps

Items that need to be addressed in the drawings sent to the NetOps team should include the following considerations. Switches will be deployed based on geographic layout of the building and disbursement of network nodes. Typically, it is not necessary to deploy a switch on every floor. Rather, hardware from adjacent floors can be connected to switches on adjacent floors, provided it is within the attenuation limitations (not to exceed 300 feet) of Cat-5e/6 cable. Access switches should always be connected via home run to Core/Distribution switches. Daisy chaining switches is strongly discouraged, however it may be approved by NetOps on a **case-by-case** basis:

- If it is cost prohibitive or not technically feasible to connect Access layer switches directly to Core/Distribution switches via home run.
- If the daisy chained switches do not exceed a maximum of 3 hops from the Core/Distribution switches.

Please note: In cases where design or budget does not allow for home runs to the core switch, project owners must sign off on risk associated with daisy chaining. Such risk include: difficulty in trouble shooting, degradation of performance and single points of failure which can all lead to increase in support costs.

- As a general rule of thumb the drawings need to show devices, locations, cabling and additionally, it should:
 - Clearly show every single IP enabled controller or component that the vendor is introducing
 - Include model information on the building automation controller or component that connects to the IP network
 - Show GSA switch and the path from each IP device to the switch location
 - Show cable runs, devices and GSA switches per floor

- Network diagrams should reference the type of cable being used. Minimum standard for Ethernet is plenum rated Unshielded Twisted Pair (UTP) Cat5e cable. Cat5e certified RJ45 (M/F) and Patch Panels to be used Cat5e cable
- Attenuation limitation is 300 feet, which is safe for data transmission
- If using a Fiber Optic riser to support intra-building network IP connectivity, detail the Type (Single or Multimode), Shielded/Armored and type of End-Point. Be sure to display how that fiber is connected through the building, and specifically which strands of fiber are being used at each connection point
- Port density requirements for GSA switches should be accurately represented
Note: Please include Sensitive But Unclassified (SBU) notice on network diagrams. See figure 2-3.

SENSITIVE BUT UNCLASSIFIED (SBU) PROPERTY OF THE UNITED STATES
COPYING, DISSEMINATION, OR DISTRIBUTION TO UNAUTHORIZED
RECIPIENTS IS PROHIBITED

Do not remove this notice
longer needed

Properly destroy or return documents when no longer needed

2.3.2 Sample Network Design Diagrams

The following is a sample depiction of an acceptable network design diagram. The vendor will need to provide an acceptable network design diagram to the NetOps before any hardware is sent to the project. Please work with your PB-ITS B&E Systems Project Manager to have your network design diagram reviewed by the NetOps team.

The following diagram (figure 2-3) illustrates a floor by floor depiction, and includes wiring and location of hardware.

2.4 Hardware Standards & Policy

All switching and routing equipment will be provided by the NetOps Team (only Government furnished equipment can be used). Only approved Government Furnished Equipment (GFE) is allowed connection (e.g., Ethernet) to the network unless specifically approved, in writing, by the Authorizing Official. Please note: NetOps does NOT provide any hardware necessary to mount the switches and routers in place. The local site needs to provide and install all items necessary to mount the hardware; such as cabinets, shelves, etc.

2.4.1 Requesting Switches and Routers

NetOps needs to be involved early in the process, when the award is made, so that they can provide switches and routers in a timely manner. Switches and routers are sent from NetOps, however the requests need to be routed through PB-ITS Building and Energy Systems Team. Once the network diagram is approved and the site's data circuit availability is confirmed, the switch(es) and the router(s) will be sent to the site. PB-ITS B&E Systems Project Manager will discuss the switching and routing needs with the various project teams before the hardware is shipped.

2.4.2 Configuration and Connection of the Switches and the Routers

The project team is expected to work with Regional GSA IT Support to physically set up the switches and routers in their designated locations. To configure a port on the switch, contact the NetOps team by submitting a Service Now Ticket for a Change Order to be created.

2.5 Acceptance of Non-Standard Hardware

All hardware designed for implementation must be scanned and approved by the GSA-IT Security prior to implementation. (See Chapter 1 "IT Policy" for details)

2.6 Implementing BACnet

2.6.1 What Is BACnet?

BACnet, by definition, is a "Data Communication Protocol for Building Automation and Control Networks" developed by the American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE). It is neither software, hardware, nor firmware. BACnet functions as a standardized set of rules that governs how computers exchange information. These rules enable the integration of control products made by different manufacturers into a single, cohesive system. While it is first being used in HVAC applications, the BACnet standard is designed to support other building control systems such as life safety, security and lighting.

2.6.2 How Does BACnet Make Use of IP Networks?

For BACnet to utilize the Internet for communication, it must speak the language of the Internet known as "Internet Protocol" or IP. IP by itself is little more than an envelope with a "from" and "to" address and a place for a message within. For equipment to communicate on the Internet a second transport layer protocol must also be used. Currently there are two primary transport layer protocols, "Transmission Control Protocol" or TCP and "User Datagram Protocol" or UDP. TCP is a reliable connection-oriented transport service that provides end-to-end reliability, re-sequencing, and flow control. Simple analogy: TCP/IP is like a telephone call providing means of communication between two parties and BACnet is the language being spoken between the two parties. UDP is a connectionless "datagram"

transport service. It is used by applications that do not require the level of service of TCP, provide the same services, or that wish to use communication services not available from TCP such as multicast and broadcast delivery. Since the BACnet protocol itself provides for the guaranteed delivery of packets, re-sequencing and flow control, it does not require the use of TCP and therefore utilizes UDP. UDP/IP was added to the BACnet specification first in Annex H.3 and later with Annex J and requires specific devices or services to be available on the BACnet network.

2.6.3 Key Definitions (BACnet)

- **BACnet Object-** The general reference to sensors, actuators, and other functional elements that make up a BACnet device. The objects fall into categories specified by BACnet protocol. Analog Input object and Analog Output object are a couple of the most commonly used objects.
- **BACnet Device-** Any device, real or virtual, that supports digital communication using the BACnet protocol. Data inside a BACnet device is organized as a series of BACnet objects. Each object has a type and a set of properties. There is always at least one object in a device – it is used to represent the device itself.
- **Device Instance-** This is the logical address that matters to BACnet. Whether on an MS/TP link or IP network, the device instance for a particular BACnet system must be unique across all subnets and routed links. There are over 4 million possible unique Device Instances based on the BACnet protocol.
- **BACnet Broadcast-** A message sent as a single unit, which may apply to more than one device.
- **Broadcast Domain-** Is the collection of available BACnet objects that can be reached by a broadcast message. With respect to IP, it is analogous to the IP subnet that one or more BACnet devices resides on. For example, in GSA, each field site may have one IP subnet that each of its building control devices resides on. A BACnet broadcast from a device on that subnet cannot communicate via a BACnet broadcast to any other BACnet device on a different IP subnet. It would require directed communication from a BACnet Router or BBMD as described below.
- **UDP/IP-** Virtually everyone has heard the term TCP/IP. This is the term often generically applied to anything Internet or anything using "standard" networking. The UDP side of the stack operates in parallel to TCP, and is automatically included in most implementations of an Ethernet based protocol stack. The difference is that TCP is considered a "connection" protocol and all communication takes place in a session that has overhead to ensure delivery of all packets. UDP is considered "connectionless", has minimal overhead, and allows the application to deal with whether the packets were delivered or not. UDP is used when data efficiency and latency is important and not data integrity nor order in which it's received. Services that uses UDP are live streaming data such as voip, video broadcast or sensor values at the moment. TCP is used when the data integrity and the order in which it's received is important. Services that use TCP is the transfer of files in which all data and the order the data is received is important, otherwise the file will be corrupted.
- **BACnet Router-** Is a BACnet device that connects two or more networks, or two or more segments of a single network.
- **BACnet Broad Cast Management Device (BBMD)-** A specialized router for BACnet broadcast messages used to forward broadcast messages between IP subnets or to

distribute broadcast messages within subnets that do not allow multicasting. In order for BACnet devices to operate as a system, they must be able to broadcast messages. However, standard IP technology dictates that routers do not forward broadcast messages. The BBMD resolves this problem by providing a re-broadcast on the local domain for any message originally broadcast on another domain. It is not necessary for all BACnet IP devices to support BBMD. Only one device on an IP domain needs to function as the BBMD. It will be configured to interact with BBMD's on other domains to provide the broadcast support. Additionally, a BBMD is capable of performing a discovery of all BACnet objects reachable to a BACnet system. This functionality is primarily what distinguishes it from a BACnet router.

- **Foreign Device-** A BACnet device that has an IP subnet address different from those comprising the BACnet/IP network which the device seeks to join. The foreign device may be a full-time node on the foreign subnet or may be a part-time participant, as would be the case if the device accessed the internet via a SLIP or PPP connection.
- **Foreign Device Registration-** In order for a foreign device to fully participate in the activities of a BACnet/IP network, the device must register itself with a BBMD serving one of the IP subnets comprising that network. "Full participation" implies the ability to send and receive both directed and broadcast messages. Each device that registers as a foreign device shall be placed in an entry in the BBMD's Foreign Device Table (FDT). The Register-Foreign-Device message from the client to the BBMD or BACnet router is always from one IP device to another.

2.6.4 Considerations and Rule Sets for Implementing BACnet on the GSA Network

- **Implementing BACnet on a Local Area Network (LAN)** This type of implementation implies that all BACnet objects and devices are located on the same IP subnet, including the server(s) that host the BACnet application(s). In GSA's case this means that the server would need to be a physical server since all virtual server infrastructure resides at a data center and therefore a different subnet. The inherent advantage of this architecture, which does not rely on the GSA Wide Area Network (WAN) for communicating BACnet messages, is that the system will not be exposed to any other BACnet system on the GSA network, and therefore cannot be negatively impacted by any other system. The disadvantages of this architecture are: 1.) It requires use of a physical server, which is against GSA's objective to consolidate application hosting to the data centers, and requires a one application per site strategy, versus the ability to support multiple sites with one server application, which reduces application licensing and infrastructure costs. 2.) Isolating BACnet systems from the network reduces potential capabilities and opportunities for data integration across a Region or the enterprise. While this approach reduces or eliminates much of the risk associated with implementing BACnet on the WAN, there is still a potential for BACnet conflicts. As mentioned, BACnet Device Instances must be unique within a BACnet system. If two or more devices possess the same instance number, this conflict will prevent one or both devices from sending and receiving BACnet messages, and can result in a BACnet broadcast storm, which may cause significant latency on the BACnet network, or its complete failure.
- **Implementing BACnet on a Wide Area Network (WAN)** This type of implementation involves a BACnet system that has one or more BACnet objects and/or devices located on a different IP subnet than the other BACnet objects and/or devices, which are part of the same BACnet system. BACnet communicates its messages either through broadcast, which can only occur within one broadcast domain, or directed communications, which involves a message being transmitted from an IP addressable device on one broadcast across the WAN to another IP addressable device on a different broadcast domain. The advantage to this architecture is essentially the opposite of confining the BACnet system to a LAN. By making use of the GSA WAN, applications can be hosted virtually, allowing sites that share a common manufacturer to leverage the same server, as well as

providing opportunities to trend and store data on a central server. Also, it is the most scalable approach that allows the creation of larger BACnet systems that may provide increased opportunities to Facilities Management related to the integration of different types of BACnet systems, such as lighting with building automation. The disadvantage to this architecture is the challenge of managing it effectively enough to avoid BACnet conflicts among different systems. And in this sense it is possible for the BACnet implementation errors from one site to negatively impact another site, perhaps even in a different region.

- There are a few primary issues to consider and things to be sure to avoid when implementing BACnet on the GSA WAN. First, similar to implementing on a LAN, it is important that all device instances associated with a BACnet network are unique. This can be particularly challenging on the GSA WAN, because a BACnet system implementer is likely not to be aware of the device instances of other BACnet systems that have devices, which may be discoverable over the GSA WAN. Although the foreign registration process provides the ability for remote devices to participate in a particular B/IP network, there may be occasions when it is desirable for two collections of B/IP devices to interoperate more closely. This type of interoperability can only produce results consistent with the assumptions and intent contained in the original BACnet standard if the configuration of the two B/IP networks has been coordinated. For example, it is assumed that device object identifiers are unique "internetwork wide." If this is not the case, the Who-Is service will produce ambiguous results. Similarly, the Who-Has service may be useless for dynamic configuration applications if multiple instances of objects with identical object identifiers exist. Second, issues can arise when BACnet objects that are not associated with each other share a broadcast domain. For example, most virtual servers supporting building control applications share the same IP subnet and many of those are BACnet applications. If those applications are broadcasting BACnet messages on across that subnet, they can be read by any other BACnet application sharing the same UDP. Since the vast majority of BACnet systems use the default UDP, this is a scenario likely to occur. In this scenario these BACnet objects are exposed to other BACnet systems.

- **Managing BACnet Device Instances**

CONSIDERATION: The previous sections detail the significance of managing device instances, regardless of the architecture or model one chooses for their BACnet system. If every BACnet device instance in use at GSA could be assigned a unique identifier, there would be very little risk for BACnet conflicts, regardless of whether they are implemented on a LAN or WAN, similar to how IP addresses are managed by any large organization, to include GSA. However, in order to implement a regime to manage device instances across the enterprise, it would be required that each building and every region that has a BACnet device in it would need to report what device instances are in use, and be able to change that device instance once a unique one was assigned. The Steering Committee considered this approach and it was deemed nearly impossible to effectively accomplish, because 100% participation would be required.

RULE: Do not duplicate device instances in any single BACnet system.

RECOMMENDATION: All regions should take inventory of their device instances and consider a regional schema and management approach to assigning device instances.

- **UDP Port Assignment**

CONSIDERATION: The standard or default UDP port number for BACnet is 47808, however, there are hundreds of UDP ports that could be used. It was agreed upon by the BACnet Steering Committee that even if BACnet objects were on the same broadcast domain, they could only communicate to each other if they were using the same UDP port number. Therefore, it was decided upon by the Committee that the full range of possible UDP ports be broken up and assigned to each region, specifically. It is

understood that most regions are already using UDP 47808 except for Region 7, which has selected a different UDP port. And while going forward, discrete UDP ports could be assigned to protect a BACnet system in one region from impacting a BACnet system in another region, existing UDP ports would need to be changed in order for this practice to be completely effective. Essentially, this allows each Region to take the initiative to protect itself from potential BACnet conflicts with systems in other regions.

RULE: 24 [unique UDP ports have been assigned to each Region](#)² per the included link. Regions are not required to change from what is likely their current UDP port, 47808, but they CANNOT USE a UDP port assigned to any other Region per the referenced distribution.

- **BACnet/Ethernet** Because Layer 2 network traffic cannot be effectively managed on the GSA network between subnets, BACnet/Ethernet is expressly prohibited from being implemented on the GSA WAN. BACnet/Ethernet can be used at a given field site, provided all BACnet devices are on the same subnet.
- **Using a BBMD**
CONSIDERATION: Each IP subnet that is part of a B/IP network comprised of two or more subnets shall have one, and only one, BBMD. Each BBMD shall possess a table called a Broadcast Distribution Table (BDT) which shall be the same in every BBMD in a given BACnet/IP network. If the BBMD has also been designated to register foreign devices, it shall also possess a Foreign Device Table (FDT).

As an example, Region 9 makes use of BBMD devices at each field site, which enables communication of BACnet messages to and from their virtually hosted application servers to and from the BACnet objects at each field site. In their configuration one of the BBMDs registers the applications server as a Foreign Device, and keeps a table of the other BBMDs in the manufactured system's BACnet network. BACnet messages to or from a specific field site, or BACnet messages to or from the server intended for BACnet objects at specific field sites must pass through and be directed by the BBMD that has registered the server as a foreign device.

RISK: During a BACnet Steering Committee meeting, a participating BACnet subject matter expert raised the point that using BBMD the way they are being used in Region 9 introduces risk, particularly if BBMDs are implemented on the subnet that hosts the virtual application server. The risk being that there could be cross communication, which could lead to BACnet storms with other BACnet systems. This expert went on to recommend that BBMDs are only necessary for initial discovery of BACnet objects, and that instead only BACnet routers are required to communicate BACnet messages from one IP subnet to another, which is required for virtually hosted application servers. It was agreed to by the committee that proper UDP port segmentation/assignment, as well as configuration of BBMD tables with specific IP addresses, would invalidate this risk. However, that assumes that integrators are aware of the IP network environment they are integrating with, and take proper care to insure these safeguards are in place. It was also recommended by both subject matter experts leading this discussion that server applications themselves, never be set up as BBMDs.

RULE: BBMDs are necessary to perform discovery of BACnet objects, and can be used to affect direct communication of BACnet messages from one IP subnet to another. Only

2

<https://docs.google.com/a/gsa.gov/spreadsheet/ccc?key=0ApuhHnPFbznqdDRPSXhyckNiRS03dV14V0ZZYlFKNkE#gid=0>

one BBMD can reside on a IP subnet. This includes the subnet that hosts the virtual servers. Due to multiple BACnet applications on virtual servers that share the same subnet, a BBMD cannot be implemented on the primary virtual server vlan. In order to implement a BBMD on a virtual server vlan two conditions must be met. 1.) The BBMD must be software based and able to be installed on a server that runs Windows Server 2008 and above 2.) A separate subnet must be created on the virtual server vlan to host the BACnet system application(s) and the software based BBMD

- **Foreign Device Registration**

RULE: A BACnet Device registered as a Foreign Device to a BBMD can only be referenced as a foreign device to one BBMD that is part of that BACnet system. For example, If a Region has a BACnet application virtually hosted that supports multiple sites that use that particular application server, you can register the server application as a Foreign Device on a BBMD at only one of the field sites. The other sites will each have one BBMD, but the Foreign Device will only be in the table of one of those BBMDs. Therefore, the BACnet messages from that server application will have to pass through the BBMD at the site that has registered the server application as a Foreign Device and then be directed to the site that BACnet message is intended for or from.

- **BACnet/IP Multicast (B/IP-M) Concept**

RULE: BACnet multicasting is another way to communicate BACnet messages from one subnet or broadcast domain to another. However, GSA does not allow multicasting over its WAN. Therefore, this approach should not be considered when configuring a BACnet system on the GSA network.

Appendix E

Contact Information

Item	Contact information
Questions relating to these policies	PB-ITS Building and Energy Systems Team pbs.pbios@gsa.gov B&E InSite ³
Enterprise Infrastructure Operations Center “EIOC”	1800-903-4472
General Support/IT Service Desk	1-866-450-5250

³ <https://insite.gsa.gov/portal/category/520178>

Chapter 3

Cabling, Data Circuit Installation and Upgrade

3.0 Overview

This chapter will provide guidance on cable installation to support the implementation of Building Monitoring and Control (BMC) Systems such as Building Automation Systems (BAS), Physical Access Control Systems (PACS), lighting control, Photovoltaic (PV) and Advanced Metering Systems (AMS). Additionally, it will establish the roles and responsibilities between vendors and GSA-IT, to ensure GSA's standards are met and questions on the agency's standards on cabling are answered. This chapter will primarily focus on guidance on Ethernet cabling, which includes Cat 5e, Cat 6 and Fiber Optic cabling for IP Based components. For questions regarding cabling for local BAS (BMC) networks, consult with the "Building Automation Systems" chapter of the Telecommunications Design and Distribution Guide. Lastly, this chapter will detail the data circuit installation process. Ultimately, this guide is related to any installations that require IP network connectivity.

3.1 Applicable Standards for Cabling Infrastructure

All cabling in GSA buildings need to be done in accordance with the BICSI standards and is in conjunction with the GSA Telecommunications Distribution and Design Guide (TDDG), as it relates to Ethernet cabling. All other types of cabling installations will be handled on a case-by-case basis.

3.2 Minimum Requirement for Ethernet Cabling

Cat 5e cabling is the minimum standard for Ethernet cabling. Please consult the Telecommunication Design and Distribution Guide (TDDG) for the latest cabling requirements as the cabling categories are rapidly changing.

3.3 Attenuation Limit

Installing the wrong network cable can result in poor signal quality, that is why following the cabling standards is very important. GSA's attenuation limit for Cat-5e/6 cable is 300 ft., beyond this length, the signal quality may become unstable and transmission errors will occur. For cable runs longer than this length, GSA-IT will likely recommend a fiber run.

3.4 How are GSA-IT's Cabling Standards Enforced?

Any cabling that will provide the medium of connection between a GSA furnished router or switch to a device that resides on the GSA LAN will be subject to a review and approval process, as specified in the TDDG, by GSA-IT. All other cabling components are to comply with Industry standards as specified in the TDDG. Any installation with GSA-provided IP address wiring back to the GSA switch, needs to follow the TDDG and the approval process. Any issues with cabling installed by the vendor will need to be addressed by the vendor that has installed the cabling. GSA IT does not assume responsibility for cabling that has not been done in accordance to TDDG and industry standards. Please ensure the vendor is held responsible to for competing work per industry standards.

3.5 Cabling Installation Options

Depending on stage and location of the BMC project, there are several approaches for cabling;

3.5.1 Cabling for New Infrastructure

For new infrastructure, the projects need to work with their controls integrator or related vendor to complete the cabling for all IP-enabled devices back to the GSA-provided network switches. Per the guidance mentioned in this chapter, GSA-IT's approval of the GSA IP network cabling design is required.

3.5.2 Cabling Infrastructure for Existing or Migrating Systems

In order to migrate an existing cabling infrastructure to a GSA-approved system, cabling may need to be redesigned. In the cases, where there is not an available contract with a vendor, Regions may work with their regional GSA-IT manager to complete this cabling. Depending on the location of the site, and the time it'll take to complete the work, arrangements for the cabling can vary, and will be handled on a case by case basis. **There are provisions in the new SAIC⁴ contract that covers cabling if the work is below a certain threshold.** Please work directly with your regional GSA-IT manager to make this determination.

Your Building and Energy Systems Tech PM can put you in contact with your regional GSA-IT manager.

Depending on the scope and requirements of the cabling work, a funding source may need to be identified by the project.

3.6 General Architecture

Please see Chapter 2 "Network Infrastructure", section 2.2 for GSA-IT's cabling requirements in a network design diagram.

3.7 Cable Installation and Support

GSA-IT encourages project managers to let vendors handle all cabling for controlling devices, metering devices and building controllers, connecting to the GSA switch. This includes serial cabling, Category 5e and Category 6 Ethernet cabling, between the building controllers and the GSA switch.

3.8 Cabling Roles and Responsibilities

- **Vendors and contractors-** Provide and install all network cabling. Please note: regions need to take measures to ensure maintenance of the control system sub-network cables, by the vendors, are stipulated in the O&M contracts.
- **GSA-IT-** Is responsible for all GSA IP traffic and will support all associated network cabling once it is installed and accepted. Will serve as the point of contact for the projects regarding proposed cabling design and questions about standards. Will work with the projects and vendors to effectively communicate standards, answer questions and provide guidance from the beginning of the design phase all the way through installation.

⁴ AAC Inc., is the vendor that handles the GSA's Technology Operations (GTO) contract (also known as the GSA helpdesk)

3.9 Overview of Data Circuit Installation

Circuit and router placement need to be considered (E.g.: the closest closet or Telecommunications Room 'TR') during the design phase to minimize any unnecessary additional cabling or having to move the circuit from the location where it was initially ordered. Circuit moves based on a mistake, from other than the telephone vendor, will incur additional charges that will be passed on to the project and will extend the delivery time of the completed circuit and sometimes push the project timeline out considerably.

3.9.1 Process for Data Circuit Requests & Sites Visits

- Data circuit installation requests are submitted via an email from the Building & Energy Technical PM for the specific region to the Requirements Analysis (RA) team at requirements.analysis@gsa.gov, to begin the ordering process.
- The email needs to contain the mailing address for the building that the circuit will terminate in, a local on-site POC, telephone number that is located in the building where the circuit will terminate (not a cell phone but a landline), requirements if users will be supported by the circuit in addition to the Building Monitoring and Control (BMC) Systems. The RA team will call the POC listed to validate all information provided and to ensure the POC is aware of the requirement so there is no confusion when the Telecommunications Carrier or the Telephone Company (known as "Telco") contacts them for access to the facility.
- The RA team for GSA-IT places an order with the telecommunications service provider for a new or an upgraded circuit at a specific location.
- The provider has 60 days from order acceptance, provided they've been given all the information they require, to have the circuit operational and ready for use. There are several definable steps that either must or can happen to deliver this circuit.
- At every location there is a Local Exchange Carrier (LEC) that has ownership of the telecommunications infrastructure at that building. If the LEC is a separate company from the one that the original order was placed with, like Verizon, then the provider will need to issue an order to the LEC to extend access from their closest point of presence to the termination point within the GSA facility.
- The 1st telco visit that will be made by a technician from the LEC will be to extend physical access from their point of presence to the appropriate termination point in the GSA facility. In some cases, the existing contractual agreements may not be in place between the service provider and the LEC, and an additional visit will need to be made by a wiring contractor to do the work necessary to extend the telecom infrastructure to the GSA facility, which would constitute a 2nd telco visit.
- Once the physical access has been completed, the service provider will need to install their Channel Service Unit/Data Service Unit (CSU/DSU) device at the point of termination to establish service. This will require a separate visit, which could be the 2nd or 3rd, depending on how many visits were required to complete the physical access.
 - Telecommunications technicians' visits should be preceded by an agreed upon notification time not less than 24 hours to the GSA point of contact that was provided to them. It is usually the building manager who serves as the point of contact, and that person may or may not be on-site already. In either case, an **ON-SITE federal employee or contractor in possession of their PIV-II Card MUST ESCORT** these

technicians through the building and to the requested access points to complete their work. Failure to meet with the Telco technician may result in the rescheduling of the visit and substantial delays of the process.

- Once service has been established, if the circuit requested was a new one, a GSA router will need to be installed at the site and connected to the (CSU/DSU). In some cases a GSA staff member will arrive on site to install the equipment, they will require access to the CSU/DSU, to complete the installation. In many cases, the router will be shipped to the building, and we will ask someone on-site to plug in the router and connect it to the CSU/DSU. There is support available in central office to walk on-site staff through the installation of the GSA router. Support for installation will be coordinated through the PB-ITS' ACT Team.

3.9.2 Important Considerations in the Circuit Installation Process

Circuit installation shall follow the guidance of the TDDG. The local POC and the installing contractor shall be aware of this requirement. Please note:

- It is crucial to identify a local point of contact that is available to meet with the vendor when they arrive on the scheduled day of visit.
- A good address for the site location is critical in this process. A physical address is not always the same as the telecommunications address. A “good address” would be an address verified from the postal service website, Google Maps or Bing Maps. Also listing any historical addresses for a location is also important. Any issues with address may affect the installation timeline.
- Circuit installation shall follow the guidance of the TDDG.

3.9.3 Circuit Installation Roles & Responsibilities

- **The Requirements Analysis Team** vets the data circuit installation requests; verifies all the provided information including the location of provided phone numbers and addresses are correct; the listed site POC is contacted and knows about the upcoming installation; collects quotes for installation and provides recommendations; and submits requests to the Telco vendor.
- **Site point of contact** is present to let vendor in the building on the scheduled site visit, confirm correct site telecommunications address and escort the Telco vendor.
- **Telco vendor** - Provides quote for circuit installation and sends order to RA for review. Subsequently they will install the circuit and help in troubleshooting connectivity issues.

Appendix F: Contact Information

Item	Contact information
Building and Energy Systems Project Managers or questions regarding policies	PBS Building IT Operations and Support Email: pbs.pbios@gsa.gov
Requirements Analysis (RA) Team	requirements.analysis@gsa.gov

Appendix G: Listing of Reference Policies

	Item	Description
G1	BICSI Standard https://www.bicsi.org/default.aspx	Worldwide association for cabling design and installation professionals.
G2	Requirements Analysis (RA) Team requirements.analysis@gsa.gov Service Now queue: GSA.CO-ENT-Requirements	In charge of managing/coordinating the data circuit installation requests; verifying all the provided information including the location of provided phone numbers and addresses are correct; the listed site POC is contacted and know upcoming installation; collecting quotes for installation and providing recommendations; and submitting requests to be processed by GSA IT
G3	The Facilities Standards for the Public Buildings Service (P100) http://www.gsa.gov/portal/content/104821	Establishes design standards and criteria for new buildings, major and minor alterations, and work in historic structures for the Public Buildings Service (PBS) of the General Services Administration (GSA).
G4	Telecommunications Distribution and Design Guide https://insite.gsa.gov/portal/content/653942	Requirements of U.S. General Services Administration (GSA) for the design and installation of telecommunications distribution systems at GSA facilities.

Chapter 4:

BMC Systems Workstations, Application Server Provisioning, Installation and Support

4.0 Overview

This chapter will provide information on hardware and software specifications provided by the GSA-IT and provide instructions for how applications should be installed; including guidance on various options when it comes to choosing a server for a project; provide comparison of physical vs. virtual server; include information on how systems are monitored by the PB-ITS Technical Operations (TechOps) team; and lastly details on what server virtualization is and how it can be implemented.

The PBS Technical Operations team is the point team when it comes to IT hardware, OS, Database and security aspects for Building, Monitoring and Control (BMC) systems projects. Requests for hardware should be routed through the Building and Energy Systems' Technical Project Manager, in Central Office. **The hosting and support of applications requires comprehensive and complete information. It is therefore critical that those stakeholders integrating these applications provide the TechOps team the required documentation as described in this chapter to enable the necessary levels of support.**

Please initiate and coordinate your project's server needs with the Building and Energy Systems Team.

4.1 About the Technical Operations Team

The TechOps Team provides the PBS organization with information technology guidance within GSA standards for BMC, National, and Regional applications.

- Hours of operation: 7am - 7pm Eastern Time
- Contact information:
 - Email - pbssystems.support@gsa.gov
 - Phone: 866-274-0781
- Forms and other information can be found here:
<http://portal.pbs.gsa.gov/webcenter/spaces/TechOps/page/BMC%20Systems>

You must use your GSA Email account to request service from the Techops team. Emails sent from corporate email accounts WILL NOT be accepted.

4.2 BMC Server and Workstations

The TechOps team keeps an inventory of BMC hardware of servers ready to be deployed to the regions. The servers have enough capacity to fit most project requirements. If your requirements are beyond the current specifications, you will need to let the Building and Energy Systems

Project Manager know ahead of time so that your project is not delayed. Projects Managers are encouraged to ask their vendors for technical explanations on why additional capacity is needed. The PBS Technical Operations team will request a solutions architecture meeting to discuss these requirements and the server build before commencing with the server deployment to ensure all aspects of the implementation adhere to GSA IT policies and infrastructure. Once the hardware order has been placed, it will take at least 15 business days in order for the hardware to be shipped to the regional GSA-IT manager's office and up to 20 business days for a server to be configured and sent to the site. Please note servers are configured at the Central Office by PB-ITS.

Building Systems Network (BSN) console/workstations are deployed by GSA-IT Desktop team, however, they are first sent to the respective regional GSA-IT manager's office to be configured and then they are shipped to the site. Once workstations are sent to the site, they are supported by the regional GSA-IT Local Support and by Building and Energy System Team's Regional Building IT Specialist (RBITS).

PLEASE NOTE: All server requests need to be routed through the PB-ITS Building and Energy Systems team. In your request, the on-site project team must provide the following:

- The application user manual for the controls product that will be installed on the server
- Point(s) of contact including address and phone to receive the server at site
- **Technical POC information for the vendor installing the server application:** Person(s) who will need administrative rights at the root level/Operating System (OS) of the server, will need to be submitted for Minimum Background Investigation (MBI). Note: At this time, temporary administrative access is granted with a preliminary favorable. Temporary access is given in 5-10 day increments.
 - Upon receiving the preliminary favorable/adjudication, the Technical POC(s) will need an ENT account, and GSA email account. This can be submitted by the project POC on ServiceNow: Service Catalog > Account Services > On-Boarding/Off-Boarding
 - Please note: Regional Project Teams need to ensure Vendor personnel maintain their ENT accounts and keep them active, in order to be able to provide technical support going forward. This includes timely completion of all tasks required to keep an ENT account active, such as annual IT Security Training courses.

4.3 Solution Architecture and Requirements Analysis

TechOps can assist project managers and vendors with planning BMC implementations that meet GSA IT standards and advise on BMC systems that have special requirements.

4.3.1 Overview of BMC Deployments

Step 1	Submit BMC Server Request Form
Step 2	Server Solutions Meeting with TechOps
Step 3	Server Configured and Security Hardened by TechOps
Step 4	Vendor installs application on Server (Administrator Rights are granted)
Step 5	TechOps Security Scans the Application for Security Vulnerabilities
Step 6	Vendor resolves Security Vulnerabilities <i>(if necessary)</i>
Step 7	TechOps Security re-scans application to ensure vulnerabilities are resolved <i>(if necessary)</i>
Step 8	Server is released to production and can be configured by vendor to add in

BMC implementation planning should begin with your regions assigned Building and Energy Systems Technical Project Manager, from Central Office. If your system will require a server, you will need to complete a BMC Server Request Form found on the [PBS Technical Operations site](#)¹. Please coordinate completing this form with your vendor and submit to your Building and Energy Systems Technical Project Manager. The TechOps technician will review the form and will schedule a discussion about the server request, and plan out the architecture with the project's stakeholders. Once all parties have agreed to a solution and a server is needed, TechOps will provide an estimated server delivery date. Standard server builds are typically completed within 15 business days. Non-standard server builds may take longer.

4.3.2 Documents to be provided by the Regional POC prior to the meeting (optional):

- BMC Server Request Form
- Application installation instructions
- Any application related documents that can contribute to the architecture design (Visio Diagram preferred)

4.3.3 Solution Architecture Meeting participants

- Regional POC(s)
- Regional technical POC (if any)
- Building manager
- Vendor technical POC, **installing the application on the server**
- Vendor assigned project managers
- TechOps team member
- B & E Project Manager
- RBITS (optional)

4.4 Server Standards

To help meet the energy efficiency goals of GSA and the move towards a virtual environment, it is standard practice for TechOps to provide VMWare virtual servers located at one of two GSA Data Centers. **Physical servers will only be provided as an exception after a full requirements evaluation done by TechOps to determine why a virtual server cannot be used.**

4.4.1 Server Virtualization

GSA uses VMware software to provide a virtual environment where multiple virtual machines run in isolation, side-by-side on the same physical server host. Each virtual machine has its own virtual hardware (e.g. RAM, CPU, NIC, hard disks, etc.) and operating system to load applications. The operating system on a virtual machine does not see the hardware components of the actual physical host or any other virtual servers that utilize the physical host's resources.

Benefits of Virtualization

- Reduced downtime - Eliminating planned downtime and preventing or reducing unplanned downtime is done through the sharing of hardware and automated restart of application servers. Properly implemented, virtualization can enable a dramatic reduction in time to recovery following a disaster.
 - If there is a failure at the VM level, the Technical Operations Team can directly respond to the failure. TechOps has multiple access paths to the VMs compared to a single connection point with a physical server at a remote office. When a physical server at a remote office fails, server downtime is dependent local network failures or having someone being dispatched to the site.
- High availability - VMware's VMotion technology enables the live migration of running

virtual machines. Virtual machines do not need to be shut down for the vast majority of physical server maintenance events. The VMware infrastructure will detect physical server failures and automatically restart VMs on another host.

- Dynamic load balancing - The VMware infrastructure automatically distributes the load across a cluster of physical servers to ensure the maximum performance of all running virtual machines.
- Hardware flexibility- Changing the resources available to a virtual machine is possible through a simple configuration change. Storage, processor, and memory resources can be added to meet demand of matched to actual resource usage throughout the lifetime of the hosted application.
- Reduced power consumption- With virtualization, a single physical server can host tens of virtual machines; this reduces the power consumed per system.
- Fast provisioning - Virtual Machines can be provisioned quickly from a template versus installing and configure a physical server.

4.4.2 Server Specifications

The latest virtual server build specifications are:

- VMWare
- Memory - 4GB
- CPU - 2 CPUs
- Hard Drive
 - System Drive - 80GB
 - Data Drive - 80GB

If your requirements are beyond the current specifications, notify your Building and Energy Systems Project Manager to avoid delays. The specifications for a new *virtual* server may be tailored to a specific requirement after a Requirements Analysis is done by TechOps. Virtual resources may also be added in the future if an application is not functioning optimally.

The latest Physical server build specifications are:

- Hardware - Dell T310
- Memory - 4GB
- CPU - 1 CPU
- Hard Drive
 - System Drive - 900 GB (RAID 5)

All server builds include the following:

- Solution architecture and requirements analysis
- Operating system installation and Security Hardening
- Database Installation and Security Hardening
- Security and compliance measures
- Server component configuration

Standard Software on GSA Servers

- Operating System
 - Windows Server 2012 R2
- Database

- Microsoft SQL 2012 R2
- Web Server
 - IIS 8.5 (Updated as Microsoft Releases)

Non-Standard / Discouraged Technologies

The following technologies are not recommended by PBS Technical Operations since they are legacy technologies which will soon not be supported.

Applications must:

- NOT use Hardware-based USB Licensing (Software Licensing should be used)
- NOT use any application that requires Java (should use HTML 5.0)
- NOT use Local Accounts (non-Active Directory) on server for application to function or be used
- NOT use additional embedded Virtual Machines

Requirements for any BMC Applications

BMC Applications, no matter which vendor, must adhere to the following requirements in order for proper functionality and support on the GSA Network.

Applications must:

- Work on VMWare in a remote data center,
- Work on the latest version of Microsoft Server Operating System (installed and managed by GSA)
- Comply with all CIS Benchmarks for Microsoft OS and Microsoft SQL hardening
- BMC software credentials shall be unique for every user

4.4.3 Server Security Hardening

Security measures are implemented on all server and applications to prevent security breaches which can result in loss of server availability or data. To that end, the TechOps Team will harden the Operating systems, Web Server, and Database with CIS Benchmarks (<https://benchmarks.cisecurity.org/downloads/benchmarks/>). In addition, after the BMC Application is installed, TechOps Security team will perform an application scan and database scan. The Security Assessment Report (SAR) will be provided to the vendor and PM on any findings from the scan. It is the responsibility of the vendor to resolve the findings as soon as possible.

All security findings not resolved within 30 days of the SAR, will be reported up to GSA IT Management and eventually up to OPM. Failure to resolve findings may result in decommission of the application.

4.5 Application Installation and Maintenance Guidelines

4.5.1 Responsibilities respective to server and application support only:

TechOps Team	Building POC
<ul style="list-style-type: none"> • Windows Component Installations • Patching for OS and DB • Resolve OS and DB vulnerabilities • Install and Configure OS and DB • Architecture Design • Provide server access • Restart Server • Monitor Application • Overall Security of Solution • Java updates 	<ul style="list-style-type: none"> • Application specific <ul style="list-style-type: none"> ○ installation ○ upgrades ○ patching ○ vulnerabilities • Application Technologies <ul style="list-style-type: none"> ○ Other Web Server ○ Any other non-OS or DB component ○ Devices

4.5.2 Application Installation Guidelines for Vendors

Do's	Don'ts
<ul style="list-style-type: none"> • Request HSPD-12 clearance, obtain Active Directory ENT Account, and GSA Email account from your GSA contacts. This is a requirement to access any GSA server. • Only expect to have temporary administrator access to the server during installation or maintenance periods. • Use the E:\ (DATA) drive to install all software on virtual servers. Physical servers will only have C:\ drive. • Request Technical Operations for reboots. • Request Technical Operations to install Windows Server Components. • Provide any documents about the software you are installing on the server to Technical Operations. • Submit server documentation after you finish installation. • Expect the server to be patched and rebooted on a monthly basis at a minimum. • Zero-Day patches will be applied immediately. • Database patching will be performed on a quarterly basis. 	<ul style="list-style-type: none"> • Do not remove the server from the ENT domain. • Do not create a local account on the server without consulting with Techops Team.. • Do not reinstall the operating system. • Do not rename the server. • Do not change the IP of the server. • Do not perform any changes related to the security policies installed or configured on the system. • Do not change file/folder permissions on the server without consulting with Techops Team.

4.5.3 Dedicated Server Support During Installation

If full attention from a TechOps server technician will be needed during the application installation, TechOps requires at least 2 weeks of advanced notice and a formal “Real-Time Support Request”. Submit an email to pbssystems.support@gsa.gov and provide date and time frame for requested support. The request must be approved by TechOps Management before real-time support can be provided.

4.6 Server Access

There are 2 types of Windows server access provided by the TechOps Team:

- **Standard User Access:** via Remote Desktop provides users the ability to run the application on the server without Administrator rights.
 - o To Request this type of access: Send an email to pbsystems.support@gsa.gov. Please note: only submit requests via GSA email addresses.
- **Administrator access:** to perform installations and upgrades. See section 4.5.3 for details.

4.6.1 Windows Server Access Requirements

Access Level	Remote Desktop User ("RDP")	Administrator
Approval required by system owner (GSA Employee)	Yes	Yes
HSPD-12 clearance required	Yes	Yes
ENT account and GSA Email required	Yes	Yes
Must be a TechOps- managed server	Yes	Yes
Duration	Unlimited	Limited to 10 business calendar days at a time (weekends and Holidays excluded)

Please see chapter 6 for server administrative and RDP access approval matrix

4.6.2 How to request Remote Desktop User Access

- Send an email to pbsystems.support@gsa.gov
- User your GSA Email account
- Specify Server Name, Users ENT account (Example: ENT\JonhASmith)

4.6.3 How to request Administrator Access

- The following guide provides detailed steps in requesting administrative access to the BMC servers:
[Temporary Admin Access to BMC Systems \(How-To Guide\)](#)⁵

4.6.4 Copying Files to a Server on the BSN

- You must use Citrix to copy files from your laptop to the server.
- You are not able to copy directly to BSN servers from Citrix or your GSA Laptop due to security restrictions.
- Please follow the process below to copy files from your local workstation to a BSN server.
- You have to access your C: Drive from within the same Citrix Windows Explorer.

⁵ <http://portal.pbs.gsa.gov/webcenter/spaces/TechOps/page/BMC%20Systems>

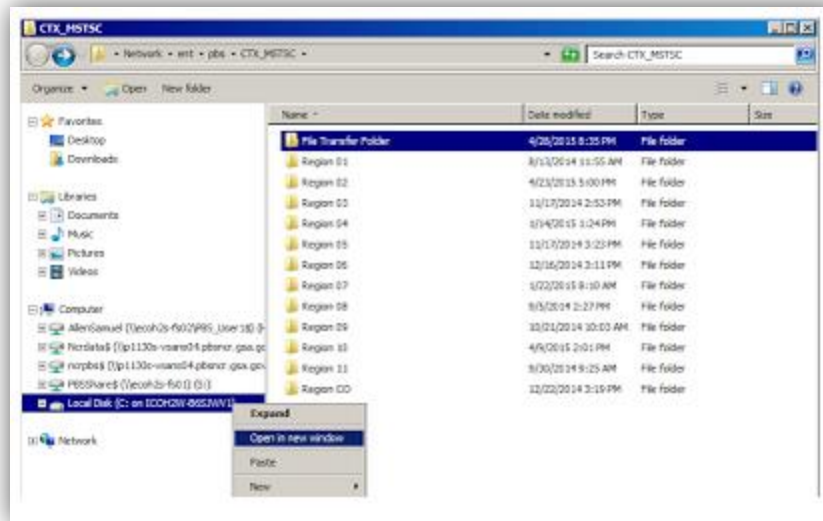


Figure 4-1

- As shown in Figure 4-1, when you launch the Citrix Shortcut 'RDP Access to BMC Servers' you get the folder structure on the right.
- Click on your respective Region and traverse the folder structure.
- On the left hand side, expand 'Computer' and **right-click** on Local Disk (C: on <yourcomputername>) and Click on 'Open in new window'.
- This will open another window with your C:\ Drive and you can copy and paste between the two windows.
- Then RDP into the server and connect to \\ENT\PBS\CTX_MSTC and retrieve the files that were uploaded.

4.6.5 Methods for Remotely Accessing a PBS Technical Operations Server

PBS servers can be accessed from Citrix or Virtual Desktop.

- **Remote Desktop Connection (RDP) to Server on GSA Network using Citrix:** For a given server, TechOps must configure a unique "RDP link" in Citrix, with the server's name and IP address, to allow remote desktop connections to that server. Citrix is generally used to access PBS servers on the BSN from GSA workstations or to access servers remotely from any computer with internet access. To request Citrix access to a server, contact the TechOps team. See link: [How to use Citrix to RDP to a Server](#)⁶.
- **Virtual Desktop Infrastructure (VDI) to Server on GSA Network:** Virtual Desktop allows the user to connect directly to the Server or launch the web application URL if the application complies with the current version of Java.

4.7 System Documentation and Monitoring

⁶<https://docs.google.com/a/gsa.gov/viewer?a=v&pid=sites&srcid=Z3NhLmdvdnxwYi1pdHMTYnVpbGRpbmctYW5kLWVuZXJneS1zeXN0ZW1zfGd4OjdjOTU4NDMzYjgxYjZkMGQ>

System documentation informs the TechOps team with the monitoring and the backups that are needed, and is also used to troubleshoot issues, and provide the proper contact names to use during an outage.

TechOps will provide monitoring and physical server backups **only if** an Application Documentation Form is completed properly and submitted to TechOps. Link: [Application Documentation Form](#)

4.7.1 Monitoring

The Technical Operation Team uses a software package named “Applications Manager” to monitor the health and availability of managed servers and applications. To ensure systems are online and functional, the monitoring software contacts the server every 5 minutes and will alert the TechOps team in the event of failure. Basic monitoring includes an availability monitor which checks to see if the server is online through ping tests every 5 minutes and can notify multiple email addresses in the event the server cannot be contacted. Advanced monitoring includes the ability to monitor services/processes/websites/databases and can take appropriate action in the event they stop or reach critical health threshold.

Monitors will only be added if the Application Documentation Form is submitted, with the exception of server health and availability monitors.

Below is a listing of the monitoring options that are offered by PB-ITS:

Windows Servers

- Server Availability
- Disk Utilization
- Memory Usage
- Service Availability Monitoring

Websites

- Availability UP/DOWN
- Average Response Time
- Page Size

Databases

- Availability UP/DOWN
- Connection Times
- Log Files
- Table Space

Database Size

- Buffer Hit Ratio
- Read, Writes, Input/output (I/O)
- SQL Statistics & Locks

4.7.2 Backup Solutions

Physical Servers	Virtual Servers
------------------	-----------------

Only files specified in BMC Application Documentation ⁷ are backed up (file size limit).	Virtual servers are entirely backed up automatically.
Backups occur Monday through Friday at 9 P.M. local time.	Backups occur Monday through Friday at 9 P.M. local time.
Daily backups are kept for up to 45 days.	Full server backups are kept for 45 days at local data center and 4 weeks off site.

4.7.3 Patching

The majority of known vulnerabilities can be solved and system attacks can be prevented by patching computers on a regular basis.

TechOps performs Windows patching on a monthly basis on the weekends. Microsoft's patch release day, occurs on the second Tuesday of each month, and is often called "Patch Tuesday". TechOps development and test server patching occurs 4 days after the patch release. Production server patching is done 2 weeks after development server patching or 18 days after Microsoft's patch release day, "2nd Tuesday".

Patching notifications are sent to all BMC email groups. The first patching notification is sent 2 weeks prior to patching and the last notification is sent the 2 days before patching .

All servers are patched every month with Windows/Microsoft Patches, Adobe Patches, and any other Windows components.

Database Patches are completed on a quarterly basis.

Email Notifications are sent to POCs, 2 weeks AND 2 days prior to the patching weekend which includes the list of servers and patches.

See Figure 4-2 for sample email that will be sent for patch notices.

⁷<http://portal.pbs.gsa.gov/webcenter/spaces/TechOps/page/BMC%20Systems>
Page 71 of 108

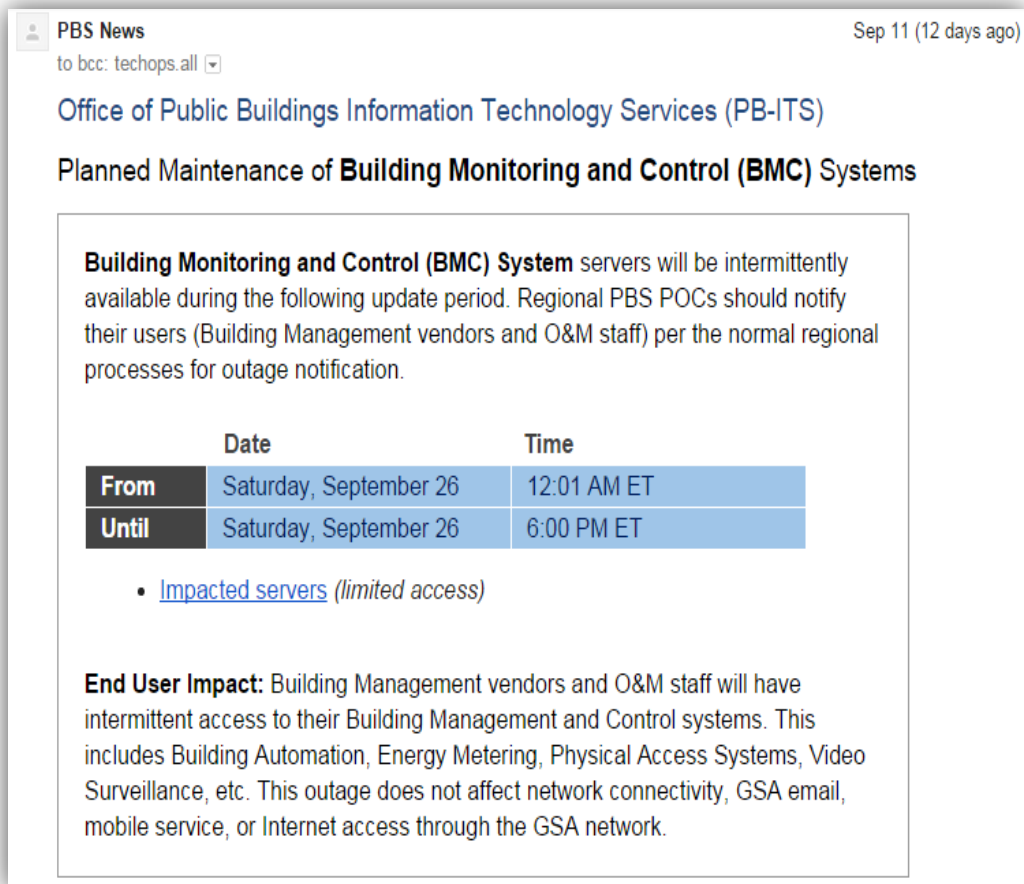


Figure 4-2

4.8 Communications

4.8.1 Planned Outages and Maintenance

Any building POC (vendors, building manager, project managers) should notify the TechOps team of planned building outages or application maintenance in advance, so the monitoring alerts can be disabled on time and unnecessary troubleshooting can be avoided.

TechOps will notify POC/Vendor listed on the below regional lists of any planned outage and include server names in the notification (if applicable). Access will only be granted to Government POCs. Please contact your B&E PM to request access. These lists also include information of the server, application installed, building affected, etc.

Region 1

https://docs.google.com/a/gsa.gov/spreadsheets/d/1K0BYJ1AEF5Yt2hF7xh_r2y1oPGbz2iwfUNS_wPFtMff0/

Region 2

<https://docs.google.com/a/gsa.gov/spreadsheets/d/1UT0ol-asxGuaPKkOeaLG3Yb7qM0EPPHyMuseNRI6qZg/edit#gid=0>

Region 3

https://docs.google.com/a/gsa.gov/spreadsheets/d/13KTHqRz98WNb_9M4O8EI3p2bTINDbrzAA_Ds_ZvHejtq/edit#gid=0

Region 4

<https://docs.google.com/a/gsa.gov/spreadsheets/d/169PsIpSManpDCOyU-WyxY3wETFWkMtUn0CpuZPbu6hE/edit#gid=0>

Region 5

https://docs.google.com/a/gsa.gov/spreadsheets/d/1DKnV60a2YfLMz5YM4xkAP4wCo_yq6ot1E5VFdmEM-RI/edit#gid=0

Region 6

https://docs.google.com/a/gsa.gov/spreadsheets/d/1YH2sj5reD8zmBTbSPdhY_l3f_OMPwmTniw_u7xCcCu6k/edit#gid=0

Region 7

https://docs.google.com/a/gsa.gov/spreadsheets/d/1T-Tb2TrtoJJ0N8D34q5UizX-18SwGQeXjhP1Hy1T_l/edit#gid=0

Region 8

https://docs.google.com/a/gsa.gov/spreadsheets/d/1q6Mqx-EF6GyAfLkrGloZyobThy8f5qcMhi0v_qVsPRM/edit#gid=0

Region 9

https://docs.google.com/a/gsa.gov/spreadsheets/d/1ETfsRdXuyJIDNIWNFNMZupgqTJ9oRNP1p_gDJEoPOJjo/edit#gid=0

Region 10

https://docs.google.com/a/gsa.gov/spreadsheets/d/1GAjilFc3r0SHu8VEn_4EWF7oYbSd7FA7zdoKCdRxwfk/edit#gid=0

Region 11

https://docs.google.com/a/gsa.gov/spreadsheets/d/1E7USKjqEEOI1QQhgYffuPjxHX_OQjdvex53cSzHLxk8/edit#gid=0

Region 12/CO

https://docs.google.com/a/gsa.gov/spreadsheets/d/1GqAY1ugaPcwlwqWfmcm9agakR0suA3Yl_O5wF65jOs8/edit#gid=0

See figure 4-3 for sample email that is sent for monthly maintenances.

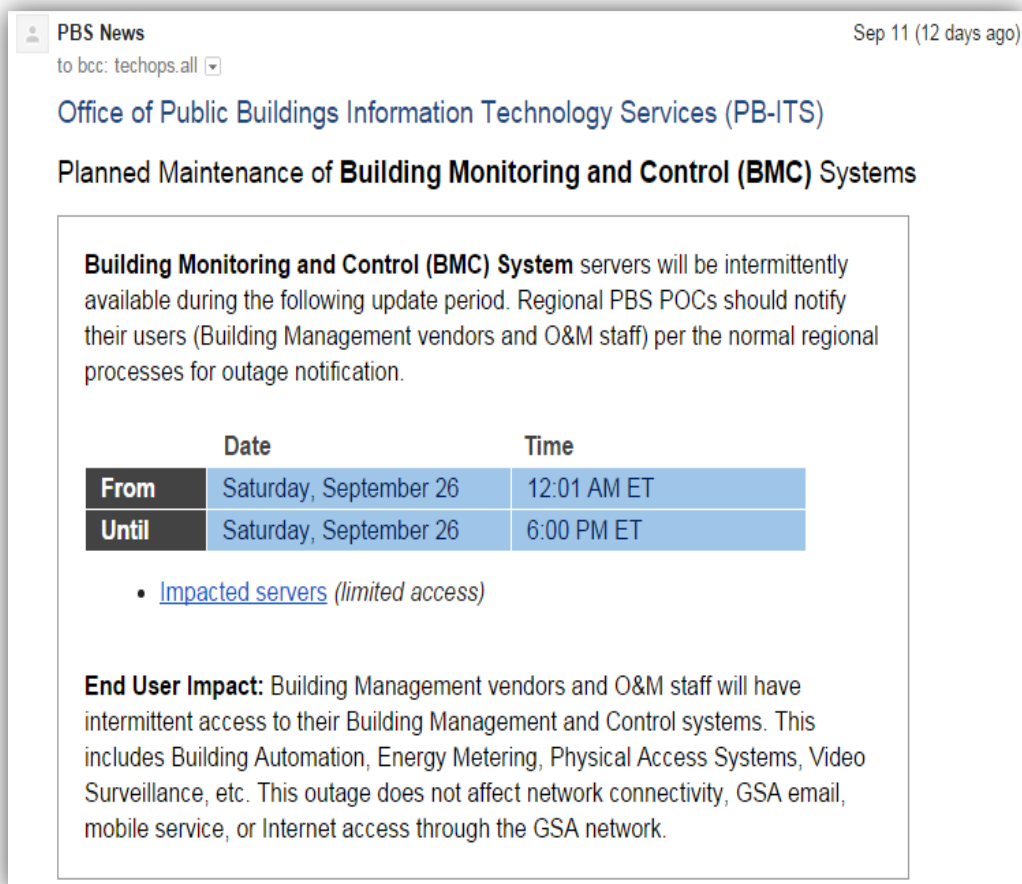


Figure 4-3

4.8.2 Unplanned outages and Maintenance

TechOps will notify POC/Vendor listed on the BAS (BMC) Application Documentation of any unplanned outage and include server names in the notification (if applicable).

If a monitor alert is generated due to an unplanned server outage, TechOps will first determine if the alert can be resolved by restarting services or rebooting the server. If the server is physical, and cannot be reached, TechOps will report the issue to IT Service Desk and site POCs and may require someone on-site to assist.

4.8.3 Group Notifications

When communicating to a mass BMC audience, TechOps will use rXX_bitna@gsa.gov contains subgroups for each region, and is maintained by the Building and Energy Team. Please reach out to your B&E Tech PM to ensure your name is added to the distribution list and you are receiving the server maintenance messages.

How to be added to Email Groups for Patching Notification:

To be added to your region's distribution group, please contact your B&E Project Manager.

Email distributions groups to where patching notifications are sent, by region:

r1_bitna@gsa.gov
r2_bitna@gsa.gov
r3_bitna@gsa.gov
r4_bitna@gsa.gov
r5_bitna@gsa.gov
r6_bitna@gsa.gov
r7_bitna@gsa.gov
r8_bitna@gsa.gov
r9_bitna@gsa.gov
r10_bitna@gsa.gov
r11_bitna@gsa.gov

To be added to your region's distribution group, please contact your B&E Project Manager.

4.9 Roles and responsibilities

- **TechOps** - Responsible for hardware, Operating System, database, backups and maintenance. (Pending documentation)
- **Building and Energy Systems Technical Project Manager** – Responsible for coordinating server requests with the regional stakeholders/business line and TechOps.
- **O&M Contractor** - Responsible for supporting the vendor-provided application and possibly the BMC equipment and advanced meters.
- **Network Operations Team (NetOps)** – Network Issues (WAN, IP Addressing, Router, Switch)
- **PBS Architecture & Circuit Tracking (ACT) Team** – responsible for circuit upgrades & Issues and slow bandwidth

Chapter 5

IT Requirements in Scopes of Work (SOWs) for Building Controls Procurements

5.0 Overview

This chapter will detail the GSA IT's requirements with respect to the procurements of Building Controls procurements at a regional level. Please work with your Contracting Officer to incorporate these requirements into the proper sections of your building controls solicitation.

5.1 Instructions

5.1.1 Use of Document

Text in grey is for reference purposes and can be changed or removed.

5.1.2 Small Projects

This documentation, which should be included on the scope of work, is to be used in any and all building controls upgrades and new procurements.

5.1.3 New Construction (Design and Construction)

This is for reference to development of Division 1 and guide specifications. For new capital construction projects, consider the following Scope of Work language for the Program of Requirements document

5.2 Scope of Work Language (to be inserted in BAS SOW)

Project Location

[Insert location name and address]

Project Points of Contact

[POC(s) Name, title, email, phone #]

Project Background

[Include detailed description of work. Eg: In recent years, building systems have advanced to more closely resemble that of IT systems given the way in which they communicate both internally and externally with other systems. As such, many of the building systems inherently utilize Internet Protocol (IP) connectivity as part of their core functionality. The General Services Administration (GSA) Public Building Services (PBS) Building Information or Control System Technology Policy mandates that all building technologies which require network or internet connectivity must utilize the GSA network. GSA's Public Buildings Information Technology Services (PB-ITS), in the office of the Chief Information Officer (CIO) is working

to integrate the building systems onto GSA's Building Systems Network (BSN). The process of implementing the BSN involves several steps during which GSA will work with building systems contractors to re-configure their devices, as necessary, for integration onto the BSN. This document is designed to specify the steps you will be required to complete for the network integration.

The facilities Building Monitoring and Controls (BMC) Systems will be upgraded to use BACnet/IP as the standard open protocol and eliminate obsolete controller hardware. The current building automation system primarily communicates using proprietary protocols on slow serial networks, and are composed of obsolete controllers. Project goals include:

- Increase the interoperability of devices, creating opportunities for energy and operational savings
- Eliminate risk associated with legacy and obsolete BAS controllers and infrastructure
- Improve accessibility to operational and energy data
- Leverage IT infrastructure to improve BMC reliability and performance]

Codes and Standards

Work shall be in accordance with the following:

- NFPA 70, National Electric Code (NEC)
- Model Building Codes (Building, Mechanical, Plumbing)
- ANSI C12.20, Class 0.5
- Facilities Standards for the Public Building Service, P-100
- Building Technologies Technical Reference Guide
- Telecommunication Design and Distribution Guide
- Federal Information Security Management Act (FISMA)
- NIST Special Publication 800-53 Rev4
- NIST Special Publication 800-82 Rev2
- GSA IT Security Procedural Guide 06-30 (Rev 8)
- IT Security Procedural Guide 08-39 (Rev 7)
- Security Language for IT Acquisition Efforts - CIO-IT Security-09-48 (Rev 2)

Reference Documents

The following references are intended to be advisory for the interpretation of the requirements in this statement of work:

- GSA New Project Smart Buildings Design and Implementation Guidelines
- [Contractor Information Worksheet \(CIW\)](#) – HSPD-12 request Form

Technical and Performance Requirements

- Security: Contractor shall comply with the requirements pertaining to mandatory HSPD-12 security clearances: The mandatory minimum security clearance level for contractor access to any GSA IT system and VPN is the preliminary adjudication of the National Agency Check with Inquiries (NACI), which is a prerequisite to acquiring ENT (GSA user domain) credentials, necessary to access any GSA furnished workstation or server.
- Users who complete HSPD-12 process will receive GSA ENT accounts for access to GSA hosted servers and workstations. Please note: per OMB mandate M-06-16 and GSA order CIO P 2181.1, "those individuals whose duties require a higher degree of trust, such as IT system administrators, those who handle financial transactions, or those who deal with PII, and other sensitive information (e.g., building drawings, etc.), will continue to require investigations associated with higher levels of trust such as the Minimum Background Investigation (MBI) or the Limited Background Investigation (LBI)." This means individuals who will need administrative access to building systems servers

will need to have an MBI clearance.

- Within 10 days of award, contractors shall submit a [CIW Form](#) for every member of the team who does not hold a HSPD-12 Clearance. See the following [page](#) for more details on the credentialing process.
- Cabling: All cabling in GSA buildings must be designed and installed in accordance with Chapter 16 (Building Automation) Building Industry Consulting Service International Inc., (BICSI) standards, for guidance on serial cables, and in conjunction with the GSA Telecommunications Distribution and Design Guide (TDDG), as it relates to Ethernet cabling
- [Schedule and Meetings: Within 10 days of contract award, the contractor's project manager shall produce a project schedule prepared in Microsoft Project or equivalent, listing all planned work activities, their duration, interdependencies, planned start and finish with a Gantt style chart. This schedule shall be continuously updated weekly until the project is complete. The project manager shall also hold a project kick-off meeting to review the schedule and update on any planned work in the upcoming weeks]
- Any required computer or server hardware (i.e. PC, laptop) and peripherals (i.e. mouse, keyboard, monitor) and/or routing and switching equipment, used to provide GSA network connectivity, will be government furnished and provided by the GSA. The BAS vendor shall not include Government Furnished Equipment, as defined, in their proposal .
 - Note: GSA IT will need to be involved in the onset discussions regarding the scope prior to award.

Project Duration

- [Include dates and if there will be options for extension. Eg: Once Notice To Proceed (NTP) has been issued, the Contractor has X calendar days to complete the controls upgrade. Extensions may be granted for unforeseen conditions and other factors outside of the Contractor's control. Requests for extensions shall be presented in writing to the Contracting Officer (CO) and shall include specific details to support the request.]

- **Engineering and Submittals**

- A network diagram of all IP-addressable devices that terminate on the GSA network shall be provided to the GSA IT PM. The GSA IT shall be included in the design phase of the network infrastructure. Vendor-provided diagrams must be submitted in digital display and in an editable format, such as Microsoft Visio.
- Any contractor- provided hardware/controllers/applications requiring access to the GSA network, must comply GSA's IT security requirements.
- All IP-enabled devices will be evaluated and scanned to determine any potential IT Security vulnerabilities. The GSA IT Security team performs security control reviews utilizing a systematic, repeatable approach, which is utilized to uniformly evaluate any device, application or general support system. Upon completion of the security review the security team is able to determine the extent to which the security controls associated with the device/application (information system) are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the established security requirements. The security team works closely with the vendor/manufacturer or the designated device POC to addresses specific actions taken or planned to correct

deficiencies in the security controls and to reduce or eliminate known vulnerabilities in the information system. Upon successful completion of the security review, GSA will have the information needed to determine the risk to agency operations, agency assets, or individuals—and thus, will be able to render an appropriate security decision for the information system. Contractors must make any required configuration changes before their product will be accepted for use. Configuration changes are not a change in scope and are not subject to equitable adjustment under the contract.

- The contractor must provide reasonable assurance to GSA that all applicable system-specific security controls are in place prior to implementing the given IT application or system, in a production environment. Current policies for assessment and authorization of systems and devices on Public Building networks are based on NIST SP 800-53 rev3. (please note: GSA IT is in transition to using FIPS 200 NIST standard to implement a tailored baseline of NIST SP 800-53 R4, using NIST SP 800-82 to assist in tailoring to address Building Monitoring and Control (BMC) devices/systems). The scanning of vendor provided hardware and software and the security evaluation can only be executed by the GSA, at this time. The IT application or system must undergo a security evaluation in order to obtain a valid Approval to Operate (ATO) signed by the Federal government. It is incumbent upon the A/E firm selected to review and understand the above-mentioned government and GSA IT security requirements. Failure to meet GSA IT requirements will be subject to liquidated damages.
- GSA will NOT accept the use of legacy technologies or systems such as:
 - Hardware-based USB/dongle Licensing (Software Licensing should be used)
 - Applications that requires Java (should use HTML 5.0)
 - Use of Local Accounts (non-Active Directory) on server for application to function or be used
 - use of additional embedded Virtual Machines
 - proprietary protocols that cannot be remediated.
 - Software that requires elevated privileges for operation (e.g., super-user or Administrator).
- All proposed standard installation, operation, maintenance, updates, and/or patching of software shall not alter the configuration settings from the approved United States Government Configuration Baseline (USGCB)
- Any Contractor proposed non-standard software must be pre-approved by GSA IT. "Nonstandard software" is defined as software which is not widely dispersed and commercially available on desktops and servers. The End-User License Agreement (EULA) needs to be made available to GSA and approved by the Office of General Counsel (OGC). The OGC reviews terms of service and determines whether or not any of the terms need to be modified or eliminated before the government can agree to the terms of service. Please see EULA fail chart below for common issues found in terms of service and what it will need to be changed to.
- Additionally, the software shall be made available to GSA to be evaluated for vulnerabilities before it's accepted for installation at GSA. The GSA standard

image utilizes a Windows operating environment, with the most current updates, as recommended by Microsoft. All software that is installed on the image is updated with the latest security patches. Contractor proposed application software and server software must be compatible with the most current version of GSA standard desktop software (i.e. Windows, Adobe, JAVA and McAfee) and server software (VMware) Vendor software shall be current in accordance with industry standards . An updated list of the version of standard currently required for GSA workstations and servers can be provided by GSA.

- All software licenses needs to be titled to GSA and should not be under the BAS vendor's ownership

	FAILS	Stock Language (Language in bold print is language to be inserted into the EULA)
1	Definition of contracting parties, typically using "You" or "You agree" language, or "if you use or install this"	<p>This language must be deleted or supplemented with the following language inserted:</p> <p>When the end user is an instrumentality of the US government, this agreement is a contract with the US Government and becomes effective when signed by the contractor and the GSA Contracting Officer as an addendum to the Contract. If this is an ID/IQ contract or Schedule Contract, ordering activities placing orders against the Schedule or ID/IQ contract are subject to this agreement as a term of the contract. This EULA (or TOS as applicable) shall bind the government, subject to federal law. This agreement shall not operate to bind a government employee or person acting on behalf of the government in his or her personal capacity.</p>
2	General Indemnity	<p>Delete the indemnity clause or supplement with:</p> <p>When the end user is an instrumentality of the US Government, the general indemnity requirement shall not apply. Recourse against the United States for any alleged breach of this agreement must be made under the terms of the Federal Tort Claims Act or as a dispute under the contract disputes clause (Contract Disputes Act) as applicable. While a dispute is pending the Contractor shall proceed diligently with performance of this contract, pending final resolution of any request for relief, claim, appeal, or action arising under the contract, and comply with any decision of the Contracting Officer.</p>
3	Patent indemnity	Contract clauses that the contractor must control any patent or other intellectual property infringement are not allowable, insofar as only the US Department of Justice is authorized to represent the US Government. This clause must be deleted, and this language inserted:

		<p>If a third party claims that products or services delivered under this contract infringes that party's patent or copyright, the contractor will indemnify the Government against liability, at the contractor's expense and pay all costs, damages, and attorneys fees that a court finally awards or that are included in a settlement approved by contractor, provided that the Government: A. Promptly notifies the contractor in writing of the claim; and B. Gives the contractor such opportunity as is offered by applicable laws, rules or regulations to participate in the defense thereof. The Government shall make every effort to permit the contractor to fully participate in the defense and/or in any settlement of such claim. However, the contractor understands that such participation will be under the control of the Department of Justice.</p> <p>Or</p> <p>When the end user is an instrumentality of the US Government, representation of the US Government in any patent indemnity action is by the US Department of Justice.</p>
4	Automatic renewals: term-limited products or services (e.g., term licenses for software, or maintenance) renew automatically, and renewal charges fall due automatically, unless the customer takes action to opt out or terminate	<p>Automatic renewals create the possibility of Anti-deficiency Act violations. This clause must be deleted, or supplemented with this language:</p> <p>When the end user is an instrumentality of the U.S. Government, automatic renewal shall not apply.</p>
5	<ul style="list-style-type: none"> • Audits 	<p>Price changing clauses: A contract that claims that one party may change the terms unilaterally is an illusory contract. This clause must be deleted.</p> <p>When the end user of this contract is an instrumentality of the US Government, discrepancies found in an audit may result in a charge by the contractor to the government user. This charge, if disputed, will be resolved through the disputes clause. The cost of the audit is paid by the contractor, not the government. Any request for audit shall be subject to applicable customer requirements pertaining to security matters, including without limitation clearances to be held and non-disclosure agreements to be executed by auditors, badging or escorting requirements for access to premises, and</p>

		other applicable requirements.
	<ul style="list-style-type: none"> • Attorney Fees & Costs • Equitable relief • Arbitration 	When the end user of this contract is an instrumentality of the US Government equitable relief, award of attorney fees, costs or interest is only allowed against when explicitly provided by statute (e.g., Prompt Payment Act or Equal Access to Justice Act.) Disputes will be resolved according to the Disputes clause, and binding arbitration will not be used.
6	Taxes	<p>FAR 29.302 states that "Generally, purchases and leases made by the Federal Government are immune from State and local taxation."</p> <p>Use this language:</p> <p>If software is licensed to an instrumentality of the US Government, any taxes to be paid by the Government as end user will be submitted to the Contracting Officer for adjudication.</p> <p>Clauses purporting to make the Government customer responsible for all taxes must be deleted from the contract. Any taxes the vendor believes to be payable by the Government should be submitted individually to the contracting officer for adjudication.</p>
7	Third Party Terms/Nested Agreements	<p>Terms provided in other EULA documents cannot bind the government unless those terms are made an attachment to the contract, which requires incorporation into the company's EULA. Incorporation by reference is not available as the content on the web is always changing.</p> <p>When the end user is an instrumentality of the US Government no license terms bind the government unless included verbatim (not by reference) in the EULA/TOS and the EULA/TOS is made an attachment to the contract.</p>
8	<p>Venue</p> <p>Arbitration</p> <p>Statute of Limitations</p>	<p>Venue and jurisdiction clauses are deleted or supplemented by the following language:</p> <p>When the end user is an instrumentality of the US Government, this is a contract with the US Government and is subject to the Federal Acquisition Regulation. Venue, jurisdiction and statute of limitations for any disputes are determined by the applicable federal statute (federal tort claims act, contract disputes act, etc.). In lieu of any provisions of this agreement requiring arbitration, the process set forth under the disputes clause shall apply.</p> <p>Arbitration clauses must be deleted. The following language may be inserted as appropriate:</p> <p>Recourse against the United States, if any, must be made under the terms of the Federal Tort Claims Act or as a dispute under the contract disputes clause (Contract Disputes</p>

		Act) as applicable. While a dispute is pending the Contractor shall proceed diligently with performance of this contract, pending final resolution of any request for relief, claim, appeal, or action arising under the contract, and comply with any decision of the Contracting Officer.
10	Equitable remedies, injunctions	<p>Clauses that indicate that company may apply or request for equitable relief are of no significance and may be retained. Clauses that indicate that the company is entitled to equitable relief in general invade the province of the trial court and must be deleted. Clauses that provide for equitable relief for copyright, trademark or patent infringement by the government are contrary to statute and must be deleted.</p> <p>When the end user is an instrumentality of the US Government, equitable relief is not available as the US Court of Federal Claims is only authorized to grant money damages as a remedy.</p>
9	Unilateral termination by contractor for breach	<p>These termination clauses must be deleted. The following language must be inserted: When the end user is an instrumentality of the US Government, recourse against the United States for any alleged breach of this agreement must be made under the terms of the Federal Tort Claims Act or as a dispute under the contract disputes clause (Contract Disputes Act) as applicable. During any dispute under the disputes clause the Contractor shall proceed diligently with performance of this contract, pending final resolution of any request for relief, claim, appeal, or action arising under the contract, and comply with any decision of the Contracting Officer.</p> <p>Or</p> <p>When the end user is an instrumentality of the US Government, recourse against the United States for any alleged breach of this agreement must be made under the terms of the Federal Tort Claims Act or as a dispute under the contract disputes clause (Contract Disputes Act) as applicable. Award of equitable relief, award of attorney fees, costs or interest is only allowed against the United States when explicitly provided by statute (e.g., Prompt Payment Act or Equal Access to Justice Act.) Disputes will be resolved according to the Disputes clause, and binding arbitration will not be used. During any dispute under the disputes clause the Contractor shall proceed diligently with performance of this contract, pending final resolution of any request for relief, claim, appeal, or action arising under the contract, and comply with any decision of the Contracting Officer.</p>
1	Unilateral modification: the	A contract that claims that one party may change the terms unilaterally is an illusory contract. This clause must be

0	vendor reserves the right to unilaterally change the license terms or terms of service, with or without notice to the customer	<p>deleted.</p> <p>This clause may be used:</p> <p>When the end user is an instrumentality of the US Government, any clause of this agreement claiming that one party to the agreement may change any terms unilaterally is of no effect.</p>
1 1	Assignment by licensor	<p>This clause must be deleted or supplemented with this language:</p> <p>When the end user is an instrumentality of the US Government, assignment of government contracts without the government's prior approval is prohibited by statute , except for assignment of payment to a financial institution.</p>
1 2	Confidentiality	<p>Schedule Contracts: Clauses that claim that the unit prices for supplies or services are confidential information must be deleted.</p> <p>When the end user is an instrumentality of the US Government, neither the EULA (this document) or the Schedule Price List shall be deemed "confidential information" notwithstanding marking to that effect.</p> <p>Notwithstanding anything in this Agreement to the contrary, the government may retain such Confidential Information as required by law, regulation or its bona fide internal document retention procedures for legal, regulatory or compliance purposes; provided, however, that such retained Confidential Information will continue to be subject to the confidentiality obligations of this Agreement.</p> <p>All other contracts: Clauses that claim that the unit prices for supplies or services are confidential information must be deleted unless the company can convince the contracting officer that release of this information would result in competitive harm.</p> <p>Insofar as the EULA terms are incorporated into the terms of the contract, the terms of the EULA are never confidential information. Clauses that claim that the EULA is confidential must be deleted.</p>

- Any contractor-proposed software solution shall require minimal administrative rights at the Operating System level. Administrative rights shall be limited for software installation, updates, patching, and in unique cases such as for troubleshooting issues. For day to day operations, the application will run with

normal user level rights. Please note: this is not in reference to full rights to the application itself, only elevated rights to the root level of the operating systems.

- Contractor shall submit disaster recover operational procedures in case of wide area network (WAN) connection loss. Disaster Recovery (DR) procedures shall ensure continued operation of the system in cases of network or server loss and shall instruction operators how to monitor and control systems in cases of internet outages
- Building Automation Installation and Configuration (Pre-Migration)
 - BAS software shall be installed and configured on GSA- provided servers.
 - GSA IT shall provide virtual servers that meet the specifications required by the BAS server software unless technical limitation prevent virtualization of the server software.
 - Client software must be installed on a GFE workstation. Any existing licenses are expected to be transferred from vendor installed workstations to the GFE workstation
 - When applicable, client software shall be loaded onto GSA- provided virtual servers. This configuration allows for flexibility in access and system control over the Building System Network.
- Building Automation Field Device Configuration (Pre-migration)
 - Every IP level device shall be configured to the proper GSA IT Building System Network IP address as directed by GSA IT
 - IP addresses for all BMC IP level devices will be issued by GSA IT and distributed after inspection and approval of network diagram
 - The BAS vendor is responsible for configuring any BACnet, UDP or TCP traffic between controllers, servers and clients to prevent “broadcast collisions” or any other network disruptions. This may include installing/configuring a BBMD or reconfiguring BACnet ports to a specified port as directed by GSA IT.
- Building Automation System Cutover (Migration)
 - Upon completion of all pre-migration work and after receipt of the government furnished network switches, the BAS contractor shall coordinate a date to “Cut-Over,” the BAS system from the existing server and onto the new BMC Server. The BAS contractor shall prepare a detailed procedure of all planned work activities, pointing out possible risks and impact to the building of all work. A risk management plan to identify risks with a planned procedure of steps to be taken if such a risk event arises shall be presented and discussed with all team members.
 - At the time of “Cut-Over,” the existing BMC network unmanaged switches (if applicable) shall be removed, replaced with new and programmed Government Furnished Switches, all network terminations shall be made, and each IP enabled device shall be migrated. Upon completion of work, documentation of any deviations shall be made on the record drawing set and published. The GSA IT department will

request various forms to be completed documenting the project which must be completed and provided within 5 business days of the cutover.

- The BAS contractor shall be required to confirm communication and functionality after completion of GSA network integration. Including device to device and device to server
 - The BAS contractor, or or GSA designee, (O&M contractor or other approved contractor) shall provide any and all cabling to GFE switches, BSN Workstations or Servers where applicable
 - At the completion of the “Cut-Over,” the existing BMC server, administrative workstations and any other unused wire, component of the BMC system shall be removed from the building and disposed of by the contractor
 - At completion of the system migration, contractor shall coordinate and verify disaster recovery operation exercise with property management and operations and maintenance staff present. This exercise shall ensure continued operations and emergency system maintenance procedures in cases of network loss.
- Work Not Included
 - Costs for providing internal GSA security escort and technical personnel
 - GSA shall ensure a connection to the GSA LAN is present and functioning
 - GSA shall provide all network switches, servers, workstations and peripherals
 - Warranty
 - Provide information of the manufacturer’s warranty including date of commissioning/startup, points of contact, 2 years parts and labor, or standard commercial (whichever is better or whichever is more comprehensive) of all components and software. The final as-builts need to be provided to GSA in a native file format (such as Visio).
 - Options
 - Please provide an additional itemized costs for this option
 - Complete exposure of building monitoring and controlling points via open protocol. This includes unrestricted access to read/write points over open protocols without additional license, or access privileges. Any required software tools, network management or device configuration shall be completed and provided for government furnished servers and workstations. Approved protocols include BACnet, LONtalk, Modbus, or OBIX.

Chapter 6

Technical Support for Building Monitoring and Control and Energy Management Systems

6.0 Overview

Due to the increasing number of sites with Building Monitoring and Control (BMC) systems being integrated with the GSA network, the end users and the support community need to be educated regarding the process to direct and manage issues and system support calls. Because the GSA helpdesk vendor⁸ is not structured to support BMC and EMS calls/issues, various groups (including the SSC⁹, building managers, O&M contractors, etc.) have coordinated and agreed to make the PB-ITS Technical Operations Team (formerly known as the PBS System Support 'PSS' Team) to act as the "command and control" point for all BMC and EMS support-related issues, directing tickets to the proper IT queue.

Property managers, project managers, energy coordinators and all other stakeholders involved in BMC projects, will work with the Technical Operations (TechOps) Team to address technical issues. This chapter outlines how BMC issues can be reported and how tickets are resolved.

6.1 Reporting a BMC Issue

Methods to report BMC issues:

- Submit an E-mail or call the TechOps team
- Call the GSA Helpdesk hotline
- Submit an IT Helpdesk ticket online with ServiceNow

Please note: There is a team within GSA, dedicated to supporting Advanced Metering System related issues. For support issues with AMS meters, send an email to the SRA Metering Support team at: AdvMeter@gsa.gov.

6.1.1 Call or Submit an Email to Technical Operations Team

You can send an email to the Technical Operations Team who will help diagnose, route or resolve your issue.

- Send an Email to pbssystems.support@gsa.gov or call 866-274-0781
- Copy your Building and Energy Systems Technical PM on emails
- Be sure to provide a detailed description of the support issue that you are having as well your contact information.

⁸SAIC (Science Applications International Corporation), is the current vendor that handles the GSA's Technology Operations (GTO) contract (also known as GSA helpdesk)

⁹ Sustainability Support Center (SSC) is the O&M/support group that handles the GSALink project.

- Please note normal hours of operation are: Monday - Friday 7 a.m. to 7 p.m. EST. Response time is up to 1 hour for emails and voicemails.
- Evening, weekends and holiday hours are: Monday - Friday 7:01 p.m. - 6:59 a.m. EST. **It is highly recommended to call and leave a voicemail.** Also, please note: evening and weekend support is limited to system outages only.

6.1.2 Call the Helpdesk hotline

You can call the helpdesk hotline and speak to a support person:

- The helpdesk hotline is **866-450-5250, option 5** “Office and Support Staff Applications,” **option 5** “Advance Metering, Building Automation and Control Systems or GSALink.”
- Be sure to include a detailed description of the support issue that you are having as well your contact information.

6.1.3 Submit an IT Helpdesk ticket online with Service Now

You can use the self-help feature of the ServiceNow ticketing system and submit an issue:

- Go to <https://gsa.service-now.com/>
- Go to Service Catalog
- Choose the option “didn’t find what you were looking for”
- Ask for the ticket to be routed to PBS National Application, “PBS NAH” queue
- Describe the issue you’re having and provide your contact information

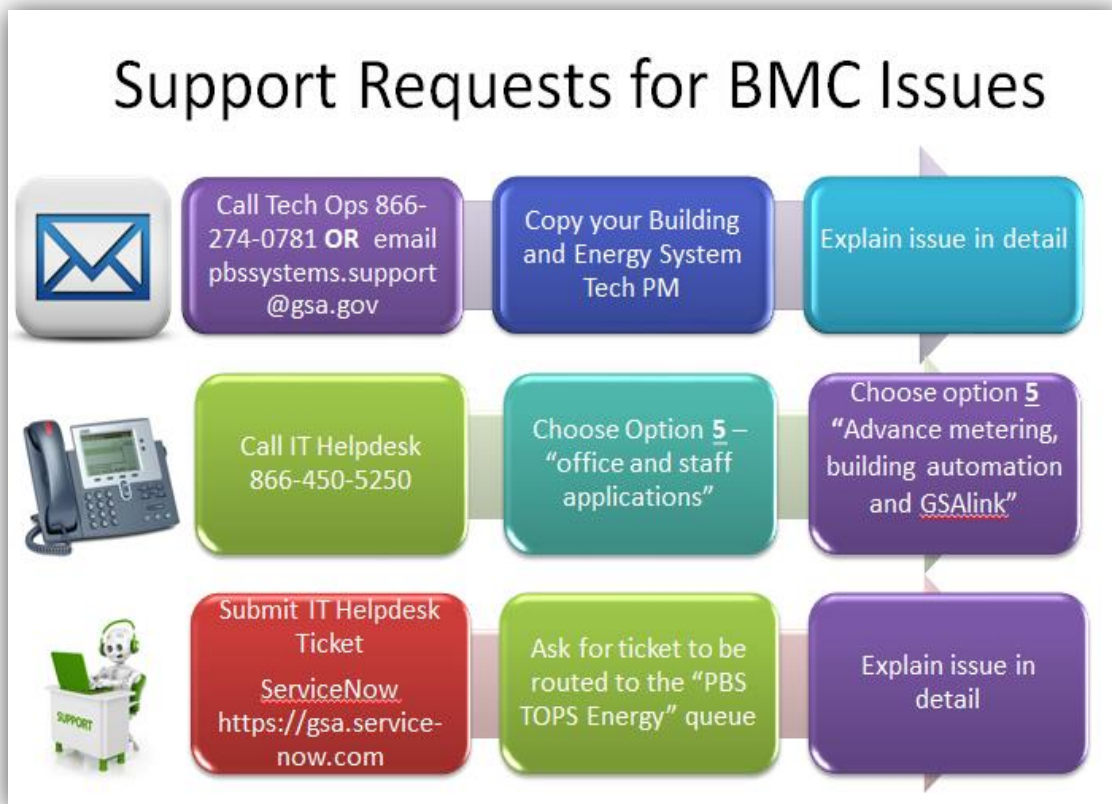


Figure 6-1: Submitting an IT helpdesk ticket to report a BMC issue

6.1.4 Describing a BMC/BAS/EMS issue

When speaking with the support agent or composing an E-mail, be sure to first mention that you are having technical problems with your “Energy Management” or “Building Monitoring & Control Systems.” Specify the type of system (i.e. Advanced Metering, Building Automation, Lighting Controls, GSALink, etc.). Do your best to describe the type of issue you are experiencing with that system. For example:

- Server name and/or IP address and/or URL
- Application Name
- Network connectivity
- Desktop/software install
- Cabling
- Requesting hardware/IPs for a site
- Circuit installation or upgrade
- Application or device accessibility from workstation, BSN Console, Citrix or VDI
- Where possible, provide a screenshot in your support request email
- Java not loading or related error

Examples of BMC, BAS or EMS applications/implementations to include on the call or E-mail

- Advanced Meter (IP based device which calculates energy usage)
- HVAC system
- NAE (BAS Appliance)
- RHEA (AMS Appliance)
- EUAS (Energy Usage Analysis System)
- NGAP (Natural GAS Acquisition Program)
- ION EEM Server (Advanced Metering Server)
- Lighting control (Part of Building Automation application)
- APOGEE (Siemens BAS Application)
- METASYS (Johnson Controls BAS Application)
- Niagara AX or Niagara 4 (N4) (Tridium BAS Application)
- Leviton (AMS Application)
- LonWorks (Networking Protocol for BAS device communication)
- Optimum Energy (BAS Application)
- HOTD (Heating Operations and Transmission District)
- TRANE (TRANE HVAC System Application)
- WEBStation-AX (Honeywell BAS Application)
- GSALink

Provide information about the site

- Building name
- Building Number
- Address, city, state

6.2 Support Process

6.2.1 Help Desk Ticket Initiation

Please see section 6.1 for details for reporting an issue. The ticket will be routed to the Technical Operations Team (TechOps), part of PB-ITS.

6.2.2 Managing and Troubleshooting Open Tickets

The TechOps Team is responsible for ownership and resolution of each ticket related to BMC

systems. They work with the ticket submitter and/or on-site point of contact to troubleshoot the reported issue.

6.2.3 Resolving Open Tickets – Roles and Responsibilities

As the TechOps team troubleshoots the ticket, it will determine which IT service organization or BMC vendor is best positioned to fix the problem. The following describes the group or organization that could be involved and in what area their support would be required.

- **PBS Technical Operations Team**

The PBS Technical Operational Team evaluates the issue and take the steps outlined in the Application Documentation (see Chapter 4).

TechOps is responsible for fixing any issues identified as hardware issues or operating system issues, including a full replacement of the hardware or operating system if necessary.

They are responsible for restoring data backups for the application.

- **GSA-IT Netops**

Provides direct support related to IP network connectivity throughout the GSA network. They coordinate with TelCo provider (Verizon) for physical network outages between the Regional Office Building and the Field Site. They support issues related to network hardware, including configuration and replacement of routers and switches.

- **Regional GSA-IT Manager**

Regional GSA-IT manager's offices supports the end user's laptop or desktop. In some cases, when resources are available, they may provide on-site technical assistance when O&M contractors/building staff members require technical assistance.

- **Building Management**

Building Manager and O&M contract staff must serve as "eyes, ears and hands" to address physical issues at the direction of the IT support services. This may include activities such as surveying cable connections, restarting/rebooting hardware, and the installation of hardware as instructed by IT support services.

- **Controls Vendor**

If it is determined that there is no issue regarding availability of GSA's IT services and infrastructure, it will be assumed that an issue resides with building control system software or hardware. The Building Manager or other on-site personnel must contact the Controls Vendor to provide full support of the application and its proprietary hardware.

- **Regional Building IT Specialist (RBITS)**

The RBITS are an extension of the GSA IT Building and Energy Systems Team, and function as the "boots on the ground". Their primary responsibilities are to support the integration activities of buildings systems to the GSA network and to provide support for production systems. The individuals in this group are often located in the Regional Office Buildings (ROB) and upon approval (from the B&E Team) can be sent to a site which is experiencing issues that GSA IT is unable to resolve remotely, and/or if local support cannot be deployed on site.

6.2.4 Closing Tickets

Tickets will not be closed until the problem has been resolved. Child tickets or separate tickets will be used to request support from other GSA IT service centers from the PBS Technical Operations team.

- **Process Flow**

The following diagram documents how BMC-related issues will be managed and resolved.

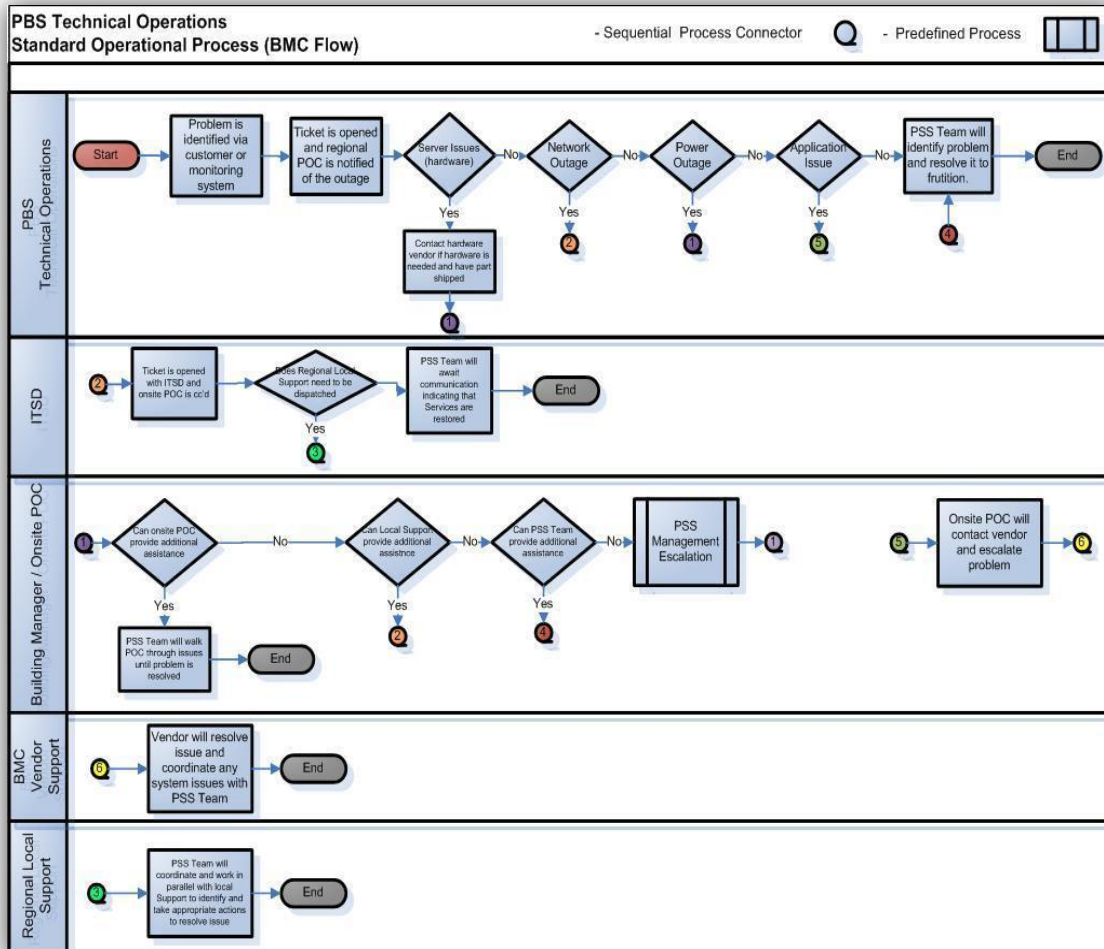


Figure 6-2: BMC support system workflow

6.2.5 BMC Outage Process

- **During business hours** (Monday - Friday, 7am - 7pm Eastern)
 - If a Server Availability outage alert is received, TechOps will immediately start to troubleshoot the issue.
 - If TechOps **is able** to restore server or service either by restarting the service or server the following actions will be taken:
 - TechOps will send an email to the Government POCs stating what was down and how it was resolved.
 - TechOps will call the listed Government POCs in order and will let the first available person know that the server was down but is now back up and will ask them to check the BMC application for functionality.
 - If restoration of the server or service **cannot** be resolved and TechOps has

exhausted all efforts, the following actions will be taken:

- TechOps will call the listed Government POCs in order and will let the first available person know that the server was down but is now back up and will ask them to check the BMC application for functionality
 - An email will be sent to the Government POCs stating what the issue is and what steps have been taken to that point.
 - TechOps may have to involve other GSA IT Teams to resolve the issue (Network Team, Server Services, vendor, etc.)
 - A request may be made by TechOps to have the software vendor help resolve the issue. It is the discretion of the Government POC if that will be allowed.
- **After business hours** (any time outside of days/hours listed above)
 - TechOps will work to restore the server or service within one hour of when an alert is received
 - TechOps will send an email to the Government POCs and peg@gsa.gov stating what was down and how it was resolved. **No phone call is necessary.**
 - If restoration of the server or service cannot be achieved by TechOps after they have exhausted all efforts,
 - TechOps will call the listed Government POCs in order and will let the first available person know what the issue is and what steps have been taken.
 - An email will be sent to the Government POCs stating what the issue is and what steps have been taken to that point.
 - TechOps may have to involve other GSA IT Teams to resolve the issue (Network Team, Server Services, vendor, etc.)
 - A request may be made by TechOps to have the software vendor help resolve the issue. It is the discretion of the Government POC if that will be allowed.

6.2.6 BMC Admin, RDP, and Reboot Process

Approval Authority Table for Administrator, RDP, and Reboot Request

Request From	Server Administrator access	Temp	Any RDP Access & Citrix App. for self or others	Server Reboot
GSA IT Team	Server POC(s) approve	Gov must	<ul style="list-style-type: none"> No Approval Needed. Request from gsa.gov email only Tech Ops will copy relevant stakeholders 	<ul style="list-style-type: none"> No Approval Needed. Request from gsa.gov email only Tech Ops will copy relevant stakeholders
ANY POC	Server POC(s) approve	Gov must	<ul style="list-style-type: none"> No Approval Needed. Request from gsa.gov email only Tech Ops will copy relevant stakeholders 	<ul style="list-style-type: none"> No Approval Needed. Request from gsa.gov email only Tech Ops will copy relevant stakeholders
Government POCs	Server POC(s) approve	Gov must	<ul style="list-style-type: none"> No Approval Needed. Request from gsa.gov email only Tech Ops will copy relevant stakeholders 	<ul style="list-style-type: none"> No Approval Needed. Request from gsa.gov email only Tech Ops will copy relevant stakeholders

Request Emails for RDP and server reboot must come from [GSA.GOV](mailto:gsa.gov) email account not Vendor email account, otherwise, GSA IT will reject the request.

6.2.7 SFTP (Secure File Transfer Protocol) Request Process

SFTP provides the ability to transfer files outside the GSA Firewall to external servers. The below described process is subject to change.

SFTP will only be allowed after a meeting is set up with a member of the TechOps Team to discuss the requirement and architecture the use of SFTP to ensure proper functionality.

Once approval is obtained, users may complete the following Google Form to request an SFTP account:

<https://docs.google.com/a/gsa.gov/forms/d/1fDHgUhQTsWTpqm6oUujPu9KMcVScZLjn9J4c3FBweUU/viewform?formkey=dFljYl9YQVWV1JFMDkzV0hZdkFzSVE6MA>

6.2.8 SMTP Email Server Information

- Simple Mail Transfer Protocol refers to the ability for applications and devices to send email notifications through the GSA email server to any email address internal or external.
- In the application or device configuration you will need to enter the following details:
 - SMTP Server:
 - smtp.gsa.gov (for use with applications and servers)
 - 159.142.67.242 (for use with devices or building consoles)
 - SMTP Port Number:
 - 25
- Authentication: No authentication is needed
- From Address: any email address with gsa.gov suffix. (For example: R2HVAC@gsa.gov)
- To Address: any valid email address you specify

Chapter 7:

Physical Access Control System (PACS)

7.1 Overview

This chapter will provide guidance on access management tools being utilized by GSA-IT. A system composed of hardware and software components that control access to physical facilities by granting/denying access based upon results from electronic validation and authentication. Physical Access Control system (PACS) is a form of access management tools consistent with governing policies. PACS is a physical access control system that utilizes contact/contactless smart-card recognition, access codes, biometrics or a combination thereof in order to gain entrance into secured areas.

Most current system compromises originate from within GSA (ENT) networks as a result of users downloading malware via spam or from a compromised site. The malware seeks to burrow deeper into systems via this “pivot point.” This aspect, in combination with the inherently sensitive nature of information (personally identifiable information (PII)) potentially accessible via PACS, requires a more robust approach to security than currently required with other Building System Controls. To this effect, a dedicated chapter was developed for these systems.

7.2 Support

7.2.1 Local Support

The local support model for these types of systems will be the same as other Building Systems Controls. GSA-IT will be responsible from the remote end of the Ethernet cabling termination back to and through the GSA network and will ensure network transport of IP traffic. The region is responsible to secure service and support for the physical system and devices that were vendor supplied.

7.2.2 Technical Operations Team

The Tech Ops team will support any server (physical or virtual) supplied by Tech Ops for any initiative related to a PACS deployment per their normal Standard Operating Procedures (SOP) and support guidelines.

Please refer to [PBS Technical Operations site](#).

7.3 Roles and Responsibilities

7.3.1 Building and Energy (B&E) System Team

The B&E team’s core roles and responsibilities for PACS will be identical to the roles and

responsibilities outlined within this guide for other Building System Controls. B&E will continue to act as the Project Manager for these efforts and will coordinate with the necessary groups for install and troubleshooting as needed. The Office of Mission Assurance (OMA), in conjunction with the HSPD-12 Governance Council, will continue to maintain oversight, provide SOPs for onboarding, migration strategies, methods of compliance, and requirements.

7.3.2 Network Operations Division (NetOps)

NetOps is responsible for providing network connectivity for the entire IP transport layer to PACS. NetOps shall provide Installation, network management and monitoring, and security and reporting services for PACS. The support services include management and monitoring of IP network switches and routers, to include physical network connections to PACS.

- **NetOps shall perform the following services:**
 - Provide design, configuration, installation, and documentation services for PACS network.
 - Coordinate configuration, testing, adjustment and implementation of PACS connections.
 - Produce and analyze network statistics for the various components of the network to determine and implement adjustments and improvements for optimized network performance.
 - Provide high level troubleshooting, fault isolation, and correction support for the PACS networks.
 - Participate in the installation, de-installation and interconnection of PACS LAN equipment as well as interconnection between WAN equipment and circuit interfaces.
 - Participate in the installation, de-installation and interconnection of PACS to the LAN interfaces.
- **Network Security**

NetOps will segment PACS on Virtual Local Area Networks (VLANs), VLANs 55 and 504 respectively, and subnets. Access to the PACS is established by use access lists. Only authorized systems included in the access list will be allowed access to PACS systems. As previously identified the differences between Building System Control systems and the need for an elevated security posture for the PACS systems that comply with the National Scope of Work dictate that they must NOT reside on the BSN and will not be able to communicate directly with any system/device(s) that are on the BSN.

7.3.3 Office of Mission Assurance (OMA)

OMA is responsible for issuance and maintenance of all agency internal documents related to the implementation of a national (enterprise wide) PACS solution. All GSA related PACS projects and/or space within GSA inventory must be fully compliant with HSPD-12, FIPS201, and Federal Identity, Credential, & Access Management (FICAM) standards. Therefore, all GSA projects will follow the *National Scope of Work (SOW) for PACS Integration/Migration* and will adhere to GSA *PACS Policy* as the guiding document for the agency's national strategy related to PACS requirements.

It will be the responsibility of OMA (with the support of GSA-IT) to ensure PACS compliance with all related and referenced policy documents.

As noted in Section 7.3.1 of this document, OMA will provide guidance on the procurement, implementation, administration and oversight for physical security countermeasures (aka "fixtures") as outlined in the *2006 GSA/FPS MOU*. Regarding O&M of PACS, OMA will work with

GSA-IT and PBS to determine the best and most cost effective approach for support. OMA will work to ensure policy or mandate changes are communicated to all stakeholders accordingly to facilitate compliance.

7.4 Network Architecture and Integration

The PACS network architecture consists of a centralized appliance and centralized certificate management piece that each Field Office Building (FOB) connects to and is integrated with. All PACS projects and integrations must meet current GSA IT policies as well as OMA and HSPD-12 Governance Council standards and policies. Each PACS project must communicate and coordinate with the regional OMA representative to ensure the PACS project meets the standards set-forth by OMA and the HSPD-12 Governance Council or run the risk of being segregated from any current or future National PACS project/program. It is required that the vendors selected to do the PACS implementation and integration be certified installers for the field devices as well as the centralized headend¹⁰ and certificate management devices. The following diagram provides the layout for the Regional network architect:

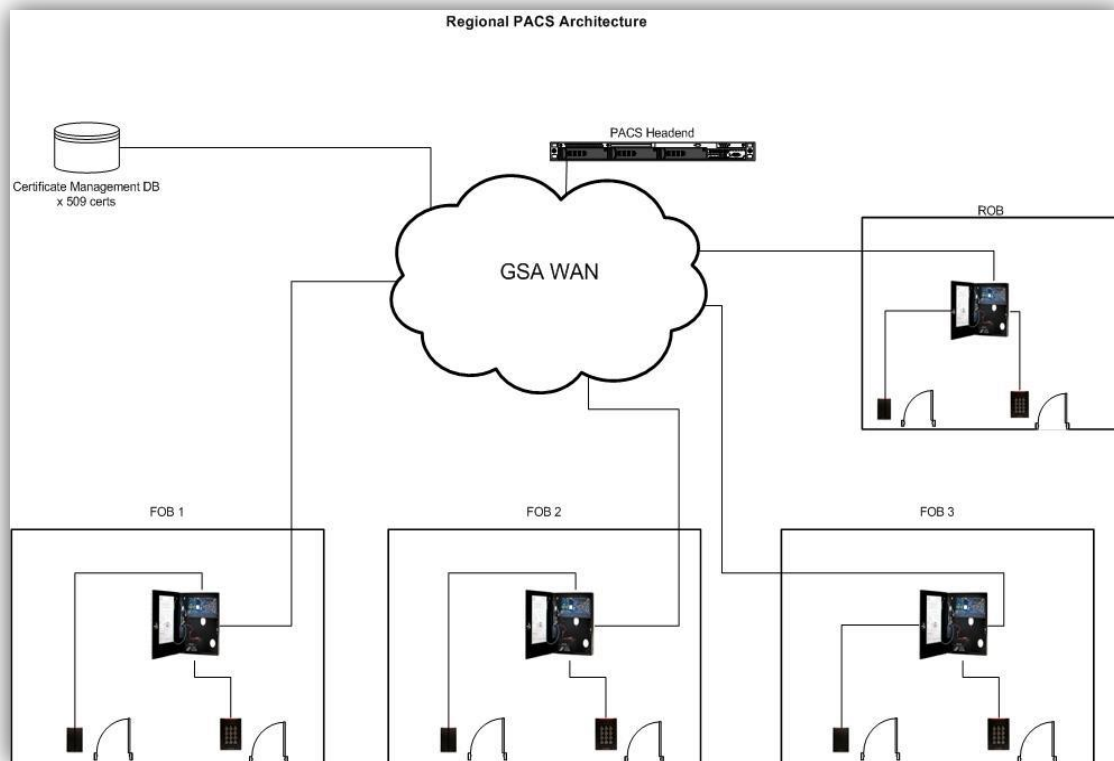


Figure 7-1: Regional PACS Architecture

7.4.1 Security Overview

All PACS devices that will be used on the GSA network will be evaluated by the PB-ITS Security team. The evaluation process will consist of security scans, a manual evaluation and the creation of a Security Assessment Report (SAR). The assessment process is detailed in *IT Security Procedural Guide: BMC DEVICE ASSESSMENTS*. For a copy of this document, please email BMC.IT.Security@gsa.gov. Refer to Chapter 1, section 5 of this guide for scan request and submittal process.

¹⁰ Head-end refers to a server based system or appliance-based system that pushes settings down to the respective readers/panels

The project activities performed by the PB-ITS security team in supporting this program include but are not limited to the activities described below. The PB-ITS Security team reviews program manager submissions and evidence, conducts independent testing, and documents all findings. The PB-ITS security team facilitates the development of and performs documentation review of articles which include:

- Vulnerability scan results
- Security Assessment Report (SAR)

The GSA IT Security team then develops reports and other required documents to complete the security function. The team then provides guidance to the PM to remediate all findings listed in the SAR.

- **Specific Security Requirements for GSA PACS Systems**
 - All PACS devices that will be implemented on the GSA network must adhere to current [GSA Security Policies](#).¹¹
 - All critical and high vulnerabilities identified must be mitigated within 30 days and all moderate vulnerabilities mitigated within 90 days or require a Acceptance of Risk to be signed by the Authorizing Official (AO).
 - All hardware must be hardened according to GSA hardening guides or CIS Level 1 benchmarks.
 - All system users must have appropriate HSPD-12 background investigations completed.
 - Systems must have on-going support to achieve or maintain an Authority to Operate, and remain in compliance with GSA Security policies.

7.5 PACS Process Flows

The following are basic process flows for PACS projects from identification through installation and integration (please note: Central Office Review Team consists of: Technical Operations Team, NetOps and PB-ITS Security):

¹¹ <https://insite.gsa.gov/portal/content/627214>

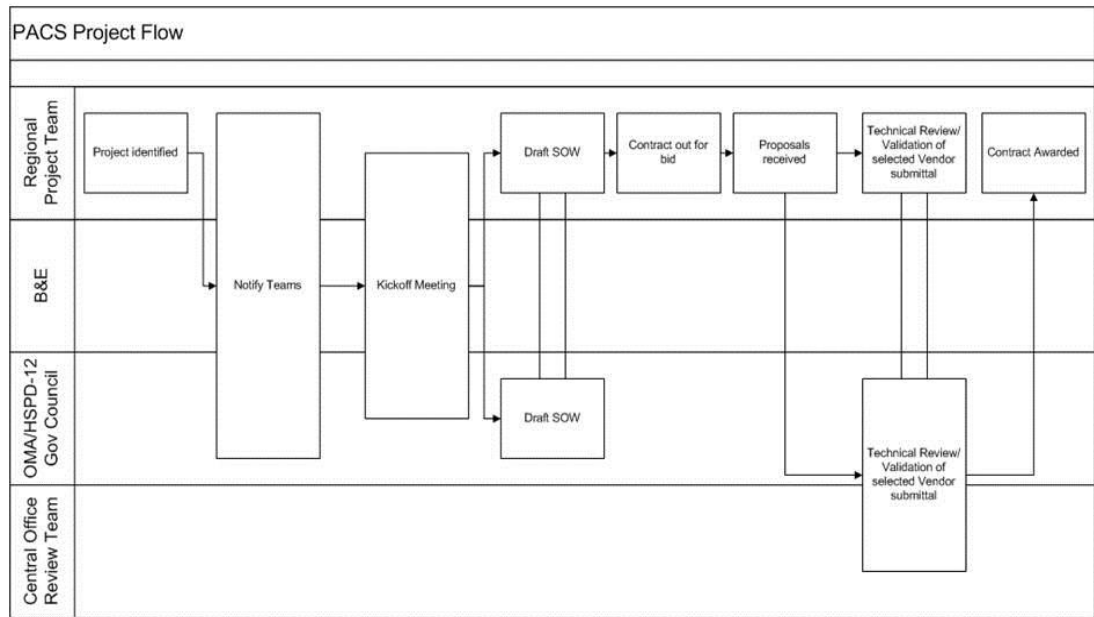


Figure 7-2: PACS Project Flow

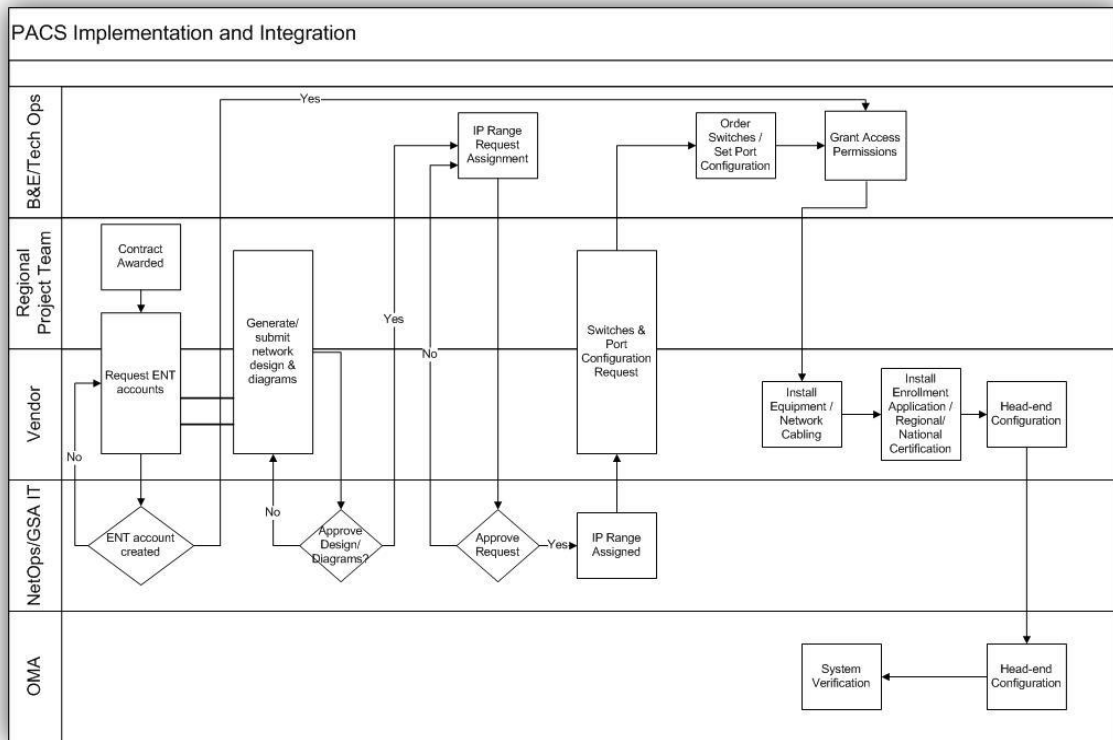


Figure 7-3: PACS Implementation and Integration

7.6 Support Tickets

Trouble tickets for these systems will follow the same flow as for all other Building, Monitoring and Control (BMC) Systems. Technical Operations Team will triage the tickets as they currently do for BMC-related issues. Please refer to Chapter 6 of this guide for further clarification/guidance.

Chapter 8

Best Practices for BMC Systems Project Implementations

8.0 Overview

This chapter was originally put together as an addendum to version 1.1 of the Building Technologies Technical Guide, due to an increasing demand to explain why GSA encourages virtualization and also to provide best practices for integration of building monitoring and control systems (BMC) to the GSA network and within its GSA's information technology (IT) environment.

8.1 Why Go Virtual?

There are several reasons why GSA IT encourages virtualization of servers to host the BMC applications:

- In 2012 an OMB directive was issued to reduce the amount of infrastructure and promote data center consolidation (DCCI).
- Executive order EO 3514, signed in October 2009 by President Obama to "to establish an integrated strategy towards sustainability in the Federal Government and to make reduction of greenhouse gas emissions (GHG) a priority for Federal agencies." This executive order is the touchstone for GSA's work in sustainability, giving GSA the responsibility and opportunity to find solutions, in partnership with other agencies to drive energy and cost savings throughout government. This EO also began our journey to the former Administrator Martha Johnsons' Zero Environmental Footprint (ZEF)
- GSA's 2010 Sustainability Plan set an agency goal for a zero environmental footprint and a 30% reduction of greenhouse gas emissions by greening the federal supply chain and creating sustainable innovation within its building portfolio. As part of ZEF, GSA IT began embracing virtualization of servers and consolidation of data centers. As part of the BMC application server virtualization effort, GSA IT leadership met with executives of large vendors such as Johnson Controls, Siemens, Honeywell, Tridium, to get their buy-in on virtualization. To this date, they have all committed to take part in this initiative.

8.2 GSA Network and Server Uptime

There are nuances associated with network "up time" in general. Rather than getting caught up in percentages and decimal points, it's important to know that GSA IT strives to have the network up and available. During an unplanned outage, the GSA IT Enterprise Infrastructure Operation

Center (EIOC), takes the lead in managing and troubleshooting the outage, with the various stakeholders. With that said, our approach should always be to have a COOP plan in place. In an event of a LAN or WAN outage, all sites need to make sure the controllers have a set default setting programmed, and have an ability to direct connect to the controllers, in order to manage the system manually. If you are unsure about what this entails, start the conversation early and talk to your Building and Energy Systems Technical PM or your Smart Buildings regional representative.

Please note: per the P100, Chapter 7, Section 7.6 Fire Alarm and Emergency Communication Systems, “With the exception of mass notification, a fire alarm and emergency communication system are not permitted to be integrated with other building systems such as building automation, energy management, security, and so on. Fire alarm and emergency communication systems must be self-contained, standalone systems able to function independently of other building systems.

8.3 Ten Tips for Running a Successful BMC Project

1. Contact your B&E Technical PM and your PBS FMSP Smart Building representative during the preparation and planning stages of the project. This will ensure that the solution is compliant with GSA security, IT, network and connectivity requirements.
 - a. Document the process used by the IT group to implement a BMC project. Be sure to incorporate the shared learning points in your project plan. Two helpful documents are the [Sample BAS Project Schedule](#) and the [Building Technologies Reference Guide](#).
2. Ensure security language and IT requirements are included in the scope of work (SOW) of the procurements. Please see chapter 5 of the [Building Technologies Reference Guide](#) for more detail.
3. Call the Technical Operations group, if you are experiencing BMC issues
Support email: pbssystems.support@gsa.gov
Direct Phone: (202) 219-0068
Hotline: (866) 274-0781
4. Include the BMC contractor, the on-site Operations & Maintenance (O&M) contractor, and other project members as specified in the [Building Technologies Reference Guide](#).
5. Before the cutover, defer to the best practices of the O&M contractor and industry standards to verify that the system is functioning properly.
6. Ensure O&M and support of the system is planned as part of the procurement process
7. Warranty of the devices, patching and security updates are included as part of procurement package.
8. Ensure network access (ENT) is maintained for the project staff
 - a. Logging into the network at least every 90 days
 - b. Changing ENT password every 90 days
 - c. Taking the annual mandatory training on the Online University (OLU)
9. Make sure to have COOP planning in place and perform a disaster recovery exercise
 - a. ensure controllers have appropriate default settings
 - b. you have an ability to direct connect to the controllers in order to manually control the system. Doing this should allow the system to be managed locally, in the event of an outage, if/when the server is not accessible.
 - c. stage a planned outage to make sure you can control the system in an event of an outage

10. Implement a GSA user training for your O&M as part of the project closeout, which will include documentation on using the system, how to contact GSA IT, how to access the system from remote, etc...

Glossary

Item	Definition
ACL 1	Access Control List (ACL) 1 is a list of all GSA Management Servers that are allowed to communicate with the servers on the BSN Server VLAN. This ACL is applied to routers managed by GSA-IT's NetOps team. The list can be found here: http://goo.gl/txh7W
ACL 2	Access Control List (ACL) 2 is a list of "legacy" servers that are allowed to communicate with the BSN Units VLAN but still remain on the GSA ENT LAN. The IPs of these servers could not be changed because of various factors. This ACL is applied to routers managed by GSA-IT's NetOps team. The list of legacy servers can be found here: http://goo.gl/vj8j5
Advanced Metering System (AMS)	An electronic system of devices that record consumption of electric energy in intervals of an hour or less and communicates that information at least daily back to the utility for monitoring and billing purposes. At GSA, most Advanced metering systems report to the national ION EEM server where the metering data is collected and monitored.
Applications	Application software, also known as an application or an "app", is <u>computer software</u> designed to help the <u>user</u> to perform singular or multiple related specific tasks. It helps to solve problems in the real world. Examples include <u>enterprise software</u> , <u>accounting software</u> , <u>office suites</u> , <u>graphics software</u> , and <u>media players</u> .
Asynchronous Transfer Mode (ATM)	ATM is a cell-based switching technique that uses asynchronous <u>time-division multiplexing</u> . It encodes data into small fixed-sized cells (<u>cell relay</u>) and provides <u>data link layer</u> services that run over <u>OSI Layer 1</u> physical links. This differs from other technologies based on packet-switched networks (such as the <u>Internet Protocol</u> or <u>Ethernet</u>), in which variable sized <i>packets</i> (known as <i>frames</i> when referencing Layer 2) are used. ATM exposes properties from both <u>circuit</u> switched and small packet switched networking, making it suitable for wide area data networking as well as real-time media transport. ATM uses a <u>connection-oriented</u> model and establishes a <u>virtual circuit</u> between two endpoints before the actual data exchange begins. ATM is a core protocol used over the <u>SONET/SDH</u> backbone of the <u>Integrated Services Digital Network</u> .
Building and Energy Systems Team	Part of the Public Buildings Information Technology Services (PB-ITS) organization, which is part of GSA IT. Responsible for integrating Building Monitoring and Control (BMC) systems onto the GSA network in an effort to facilitate reliable and secure network services and system application support. This includes all efforts related to the technical integration and support of our business line customers,

	particularly those related to the Smart Buildings program within the Facilities Management division of PBS.
Building Automation System (BAS)	<p>The computer networking of electronic devices designed to monitor and control the HVAC, humidity control, ventilation and lighting systems in a building.</p> <p>For consistency reasons, the term “BMC” is used to encapsulate various automation systems at GSA. Please see definition below.</p>
Building Monitoring and Controls Systems (BMC)	BMC systems include, but are not limited to building technologies such as advanced metering systems (AMS), building automation systems (BAS), lighting control systems, physical access control systems (PACS), renewable energy systems, and kiosks.
Building Systems Network (BSN)	BSN is a strategy which uses a virtual network within the GSA physical network to isolate Building Monitoring and Control systems from the GSA ENT domain. It is implemented through a Virtual Local Area Network (VLAN) as applied on network switches and an Access Control List (ACL) as applied on network routers to segment the IP communications from your building control system application(s) and devices from the rest of the GSA business network, aka the ENT domain.
BSN Console	BSN Building Consoles are GSA workstations (desktops or laptops) that receive a standard GSA image, but which are not joined to the ENT domain the way normal GSA user workstations are. This means that they do not receive the same group policies, and do not adhere to the same IT security standards that a user's ENT workstation does. It also means that Building Consoles cannot communicate or interface with any sites or services that are available or that are made available by the ENT domain. This includes, but is not limited to GSA email, GSA, gov, the public internet, etc. The only thing that the Building Console can communicate to are building system application servers, and building system IP-based controllers, if those devices have a web or RDP interface. The Building Console and its communication restrictions are illustrated in the figures above.
BSN Server VLAN	Building System Network (BSN) Server VLAN is a logical network separation within the GSA Network to isolate BSN Servers from the GSA ENT network and the BSN Units VLAN. This VLAN can communicate to all servers within the BSN Server VLAN and all devices and building consoles on the BSN Units VLAN. GSA Management Servers on the ENT network can communicate to the BSN Server VLAN via ACL 1. By default, all new BMC Servers are placed in this VLAN.
BSN Units VLAN	Building System Network (BSN) Units VLAN is a logical network separation within the GSA Network to isolate BSN Devices and Building Consoles from the GSA ENT network. This VLAN can communicate to all building devices within the VLAN and the BSN Server VLAN and the legacy BMC Servers located on ACL 2.
Coaxial cable	Is the kind of copper cable used by <u>cable TV</u> companies between the community antenna and user homes and businesses. Coaxial cable is sometimes used by telephone companies from their central office to the telephone poles near users. It is also widely installed for use in business and corporation <u>Ethernet</u> and other types of <u>local area network</u> .

CSU	Channel service unit used to connect to digital leased lines on the line side.
Devices	Something, as a machine, devised for a particular function: apparatus, appliance, contraption, contrivance.
DSU	Digital service unit is <u>telecommunications</u> circuit terminating equipment used to connect to digital leased lines on the LAN side.
DTS	Dedicated Transmission Service
Energy Management Systems (EMS)	Used interchangeably with BMC. Please see def for BMC.
ENT	GSA Enterprise Domain
Ethernet	Network architecture that uses carrier-sense multiple-access with collision detection (CSMA/CD) for controlling access to the network media and baseband broadcasts. It uses star topology.
FIPS 140-2	Federal Information Processing Standard (FIPS) is a certification that specifies the exact module name, hardware, software, firmware, and/or applet version numbers. Encryption is an important tool used to meet security control requirements. When used to protect sensitive information Federal systems must use encryption that meets the requirements of the Federal Information Processing Standard (FIPS) 140-2. Once a system has been designed and deployed using FIPS compliant technologies it must be operated following documented procedures to ensure keys are created, stored, retired, revoked and otherwise managed in a consistent and secure manner. The National Institute of Standards and Technology (NIST) promulgated FIPS 140-2 to ensure that encryption technology meets minimum standards when protecting sensitive data on Federal networks and systems. All cryptographic modules used in Federal systems must meet the standards in FIPS 140-2. FIPS 104-2 provides a certification path for vendors of cryptographic modules. Certification ensures that the standards are met in the specific vendor implementation. Wireless and SFTP (Secure File Transfer Protocol) Data Transmissions also need to meet FIPS 140-2 protocol. (See FIPS 140-2 http://insite.gsa.gov/graphics/staffoffices/keymgmt.doc)
FTP	Transport Protocol is used to transfer files between computers.
GEMS/GNNI	GSA Electronic Messaging Services
GFE	Government Furnished Equipment
NetOps	Internetworking and Security Services. Part of the GSA IT. Manages the wide and local area networks (GSA WAN and LAN) and provides network security management for GSA infrastructure to include firewalls, intrusion detections and virus detection systems
Intranet	Refers to using internet technologies such as a web server on an internal network.
IP	Internet Protocol OS used for software addressing of computers and works at the data link layer. RFC 791
ISP	Internet Service Provider

LABN	Local Area Backbone Network
LAN	Local Area Network
MAC	Media Access Control address. Basically a network card unique hardware address.
MBI	Minimum Background Investigation
MPLS	GSA's Multi-Protocol Label Switching Backbone
Network Operations Center (NOC)	A center from which network monitoring and control, or network management, is exercised. At GSA the NOC controls and manages the network and the network switches. Part of the GSA-IT group
NACI	National Agency Check with Inquiries
OCIO	Office of the Chief Information Officer. With the IT consolidation, the office of PB-ITS (formerly known as PBS CIO) and OCIO are now referred to as GSA-IT.
Optical fiber	Also known as "fiber optic" refers to the medium and the technology associated with the transmission of information as light pulses along a glass or plastic strand or fiber. Optical fiber carries much more information than conventional copper wire and is in general not subject to electromagnetic interference and the need to retransmit signals. A type of fiber known as <u>single mode fiber</u> is used for longer distances; <u>multimode fiber</u> is used for shorter distances.
Physical Access Control System (PACS)	A control system that utilizes contact/contactless smart-card recognition, access codes, biometrics or a combination thereof in order to gain entrance into secured areas.
PBS CIO	Public Building Service Chief Information Office. This is the old organizational name for PBS IT Services 'PB-ITS', which is now part of GSA-IT.
PB-ITS	Public Buildings Information Technology Services (formerly known as PBS CIO)
PBS NAH	PBS National Applications. This is a queue in the ServiceNow tickets systems and is monitored by the PBS Technical Operations Team who oversees and handles BMC related support issues and manages server deployment and support.
RAS	Remote Access Service (RAS) with Windows NT allows users connecting to the network using a modem to use network resources.
Requirements Analysis (RA) team	In charge of managing/coordinating the data circuit installation requests; verifying all the provided information including the location of provided phone numbers and addresses are correct; the listed site POC is contacted and know upcoming installation; collecting quotes for installation and providing recommendations; and submitting requests to be processed by GSA IT
ROB	GSA's Regional Office Buildings
Router	Routes data packets between two networks. It reads the information in each packet to tell where it is going.

SAIC Applications International Corporation) (Science	Is the vendor that handles the GSA's Technology Operations (GTO) contract (also known as GSA helpdesk)
SOW	Statement of work.
STP	Shielded Twisted Pair cable. 100 meter maximum length. 16-155 Mbps speed. Lower electrical interference than UTP.
TCP	Transport Control protocol is a connection oriented reliable protocol working at the transport layer. RFC 793.
Topology	The shape of the physical connection of a network with regard to repeaters and networked computers. The three main types are ring, bus, and star.
Twisted pair	Twisted pair is the ordinary copper wire that connects home and many business computers to the telephone company. To reduce crosstalk or electromagnetic induction between pairs of wires, two insulated copper wires are twisted around each other. Each connection on twisted pair requires both wires. Since some telephone sets or desktop locations require multiple connections, twisted pair is sometimes installed in two or more pairs, all within a single cable. For some business locations, twisted pair is enclosed in a shield that functions as a ground. This is known as shielded twisted pair (STP). Ordinary wire to the home is unshielded twisted pair (UTP).
UTP	Unshielded Twisted Pair cable. Normally UTP contains 8 wires or 4 pair. 100 meter maximum length. 4-100 Mbps speed.
VPN	Virtual Private Networking. The function of VPN is to allow two computers or networks to talk to each other over a transport media that is not secure, but the network is made secure by VPN security protocols.
WAN	Wide Area Network is larger than a MAN and may be an enterprise network or a global network.
WLAN	Wireless local area network (WLAN) links two or more devices using some wireless distribution method (typically <u>spread-spectrum</u> or <u>OFDM</u> radio), and usually providing a connection through an access point to the wider internet. This gives users the mobility to move around within a local coverage area and still be connected to the network.
Workstation	Workstation is a high-end <u>microcomputer</u> designed for technical or scientific applications. Intended primarily to be used by one person at a time, they are commonly connected to a <u>local area network</u> and run <u>multi-user operating systems</u> . The term <i>workstation</i> has also been used to refer to a <u>mainframe computer</u> terminal or a PC connected to a <u>network</u> .